

DOCKET NO.: 255635US6PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Satoshi KITANI, et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HERewith

INTERNATIONAL APPLICATION NO.: PCT/JP03/16226

INTERNATIONAL FILING DATE: December 18, 2003

FOR: MUTUALLY AUTHENTICATING METHOD, PROGRAM, RECORDING MEDIUM,
SIGNAL PROCESSING SYSTEM, REPRODUCING APPARATUS, AND INFORMATION
PROCESSING APPARATUS

REQUEST FOR PRIORITY UNDER 35 U.S.C. 119
AND THE INTERNATIONAL CONVENTION

Commissioner for Patents
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

COUNTRY
Japan

APPLICATION NO
2003-006915

DAY/MONTH/YEAR
15 January 2003

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP03/16226. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Gregory J. Maier
Attorney of Record
Registration No. 25,599
Surinder Sachar
Registration No. 34,423

Customer Number

22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

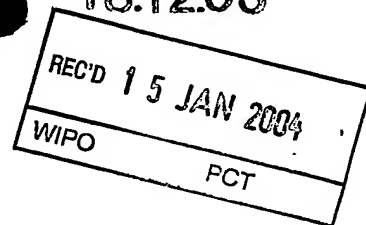
BEST AVAILABLE COPY

S04 P0076 W U U U

PCT/JP03/16226
Rec'd PCT/PTC 31 AUG 2004

18.12.03

日本国特許庁
JAPAN PATENT OFFICE



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 1月15日
Date of Application:

出願番号 特願2003-006915
Application Number:
[ST. 10/C]: [JP2003-006915]

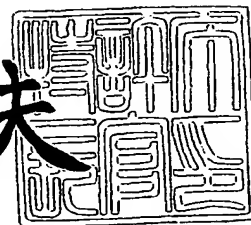
出願人 ソニー株式会社
Applicant(s):

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2003年11月 7日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



BEST AVAILABLE COPY

出証番号 出証特2003-3092309

【書類名】 特許願

【整理番号】 0290782806

【提出日】 平成15年 1月15日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 H04N 5/85

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 木谷 聡

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 村松 克美

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100082762

【弁理士】

【氏名又は名称】 杉浦 正知

【電話番号】 03-3980-0339

【選任した代理人】

【識別番号】 100120640

【弁理士】

【氏名又は名称】 森 幸一

【手数料の表示】

【予納台帳番号】 043812

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0201252

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 相互認証方法、プログラム、記録媒体、信号処理システム、再生装置および情報処理装置

【特許請求の範囲】

【請求項 1】 不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、上記再生装置が上記コンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法において、

上記再生装置は、当該再生装置を表す情報と上記リボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第 1 の判定ステップを有し、

上記情報処理装置は、当該情報処理装置を表す情報と上記リボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第 2 の判定ステップを有し、

上記第 1 の判定手段によって無効化すべきという判定をされなかった場合に生成される第 1 の鍵情報と、上記第 2 の判定手段によって無効化すべきという判定をされなかった場合に生成される第 2 の鍵情報とを用いて、上記再生装置と上記情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法。

【請求項 2】 請求項 1 において、

上記相互認証ステップは、

上記情報処理装置が上記伝達手段を介して正常に動作しているかを上記再生装置において確認する第 1 の確認ステップと、

上記再生装置が上記伝達手段を介して正常に動作しているかを上記情報処理装置において確認する第 2 の確認ステップとを有することを特徴とする請求項 1 に記載の相互認証方法。

【請求項 3】 請求項 2 において、

上記再生装置は、

乱数を生成する第 1 の乱数生成ステップと、

所定の計算をする第 1 の計算ステップとを有し、

上記情報処理装置は、

乱数を生成する第2の乱数生成ステップと、

所定の計算をする第2の計算ステップとを有し、

上記第1の確認ステップは、

上記第1の乱数生成ステップにより生成される第1の乱数と、上記第2の乱数生成ステップにより生成される第2の乱数とを上記伝達手段を介して上記再生装置と上記情報処理装置との間で相互に交換する第1の乱数交換ステップと、

上記再生装置において、少なくとも上記第1の鍵情報と上記相互に交換された第1の乱数および第2の乱数とを用いて上記第1の計算ステップにより計算した結果と、上記情報処理装置から上記伝達手段を介して送られた、少なくとも上記第2の鍵情報と上記相互に交換された第1の乱数および第2の乱数とを用いて上記第2の計算ステップにより計算した結果とが同一であることを比較する第1の比較ステップとを有し、

上記第2の確認ステップは、

上記第1の乱数生成ステップにより生成される第3の乱数と、上記第2の乱数生成ステップにより生成される第4の乱数とを上記伝達手段を介して上記再生装置および上記情報処理装置との間で相互に交換する第2の乱数交換ステップと、

上記情報処理装置において、上記再生装置から上記伝達手段を介して送られた、少なくとも上記第1の鍵情報と上記相互に交換された第3の乱数および第4の乱数とを用いて上記第1の計算ステップにより計算した結果と、少なくとも上記第2の鍵情報と上記相互に交換された第3の乱数および第4の乱数とを用いて上記第2の計算ステップにより計算した結果とが同一であることを比較する第2の比較ステップとを有していることを特徴とする相互認証方法。

【請求項4】 不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、上記再生装置が上記コンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法のプログラムであって、

上記再生装置は、当該再生装置を表す情報と上記リボケーション情報とを用い

て当該再生装置を無効化すべきか否かを判定する第1の判定ステップを有し、

上記情報処理装置は、当該情報処理装置を表す情報と上記リボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第2の判定ステップを有し、

上記第1の判定手段によって無効化すべきという判定をされなかった場合に生成される第1の鍵情報と、上記第2の判定手段によって無効化すべきという判定をされなかった場合に生成される第2の鍵情報とを用いて、上記再生装置と上記情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法のプログラム。

【請求項5】 不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、上記再生装置が上記コンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法のプログラムを格納した記録媒体であって、

上記再生装置は、当該再生装置を表す情報と上記リボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第1の判定ステップを有し、

上記情報処理装置は、当該情報処理装置を表す情報と上記リボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第2の判定ステップを有し、

上記第1の判定手段によって無効化すべきという判定をされなかった場合に生成される第1の鍵情報と、上記第2の判定手段によって無効化すべきという判定をされなかった場合に生成される第2の鍵情報とを用いて、上記再生装置と上記情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法のプログラムを格納した記録媒体。

【請求項6】 不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、上記再生装置が上記コンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置とを備える信号処理システムであって、

上記再生装置は、当該再生装置を表す情報と上記リボケーション情報とを用い

て当該再生装置を無効化すべきか否かを判定する第1の判定手段を有し、

上記情報処理装置は、当該情報処理装置を表す情報と上記リボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第2の判定手段を有し、

上記第1の判定手段によって無効化すべきという判定をされなかった場合に生成される第1の鍵情報と、上記第2の判定手段によって無効化すべきという判定をされなかった場合に生成される第2の鍵情報とを用いて、上記再生装置と上記情報処理装置とが相互に認証する相互認証手段と、

上記相互認証手段による相互認証後に、上記再生装置および上記情報処理装置に共通の共通鍵を生成する共通鍵生成手段とを備えることを特徴とする信号処理システム。

【請求項7】 請求項6において、

上記相互認証手段は、

上記情報処理装置が上記伝達手段を介して正常に動作しているかを上記再生装置において確認する第1の確認手段と、

上記再生装置が上記伝達手段を介して正常に動作しているかを上記情報処理装置において確認する第2の確認手段とを有することを特徴とする信号処理システム。

【請求項8】 請求項7において、

上記再生装置は、

乱数を生成する第1の乱数生成手段と、

所定の計算をする第1の計算手段とを有し、

上記情報処理装置は、

乱数を生成する第2の乱数生成手段と、

所定の計算をする第2の計算手段とを有し、

上記第1の確認手段は、

上記第1の乱数生成手段により生成される第1の乱数と、上記第2の乱数生成手段により生成される第2の乱数とを上記伝達手段を介して上記再生装置と上記情報処理装置との間で相互に交換する第1の乱数交換手段と、

上記再生装置において、少なくとも上記第 1 の鍵情報と上記相互に交換された第 1 の乱数および第 2 の乱数とを用いて上記第 1 の計算手段により計算した結果と、上記情報処理装置から上記伝達手段を介して送られた、少なくとも上記第 2 の鍵情報と上記相互に交換された第 1 の乱数および第 2 の乱数とを用いて上記第 2 の計算手段により計算した結果とが同一であることを比較する第 1 の比較手段とを有し、

上記第 2 の確認手段は、

上記第 1 の乱数生成手段により生成される第 3 の乱数と、上記第 2 の乱数生成手段により生成される第 4 の乱数とを上記伝達手段を介して上記再生装置および上記情報処理装置との間で相互に交換する第 2 の乱数交換手段と、

上記情報処理装置において、上記再生装置から上記伝達手段を介して送られた、少なくとも上記第 1 の鍵情報と上記相互に交換された第 3 の乱数および第 4 の乱数とを用いて上記第 1 の計算手段により計算した結果と、少なくとも上記第 2 の鍵情報と上記相互に交換された第 3 の乱数および第 4 の乱数とを用いて上記第 2 の計算手段により計算した結果とが同一であることを比較する第 2 の比較手段とを有していることを特徴とする信号処理システム。

【請求項 9】 請求項 8 において、

上記共通鍵生成手段は、

上記第 1 の乱数生成手段により生成される第 5 の乱数と、上記第 2 の乱数生成手段により生成される第 6 の乱数とを上記伝達手段を介して上記再生装置と上記情報処理装置との間で相互に交換する第 3 の乱数交換手段と、

上記再生装置において、少なくとも上記第 1 の鍵情報と上記第 5 の乱数と上記第 6 の乱数とを用いて上記共通鍵を生成する第 1 の共通鍵生成手段と、

上記情報処理装置において、少なくとも上記第 2 の鍵情報と上記第 5 の乱数と上記第 6 の乱数とを用いて上記共通鍵を生成する第 2 の共通鍵生成手段とを有することを特徴とする信号処理システム。

【請求項 10】 請求項 9 において、

上記伝達手段を介して、上記共通鍵を用いた共通鍵暗号方式で上記再生装置から上記情報処理装置へ情報を送る第 1 の送信手段と、

上記再生装置において、上記第1の鍵情報と上記記録媒体固有の情報を用いて記録媒体固有の鍵情報を生成する中間鍵情報生成手段とを備えることを特徴とする請求項7に記載の信号処理システム。

【請求項11】 請求項10において、

第3の鍵情報を、少なくとも上記記録媒体固有の鍵情報を用いて暗号化する鍵情報暗号化手段と、

上記鍵情報暗号化手段により暗号化された上記第3の鍵情報を上記記録媒体に記録する暗号化鍵情報記録手段と、

上記第3の鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成手段と、

上記コンテンツ情報暗号化鍵を用いて暗号化されたコンテンツ情報を上記記録媒体に記録するコンテンツ情報記録手段とを備えることを特徴とする信号処理システム。

【請求項12】 請求項11において、

上記鍵情報暗号化手段、上記暗号化鍵情報記録手段、上記最終暗号化鍵生成手段、上記コンテンツ情報記録手段は、

上記情報処理装置が有しているとともに、

上記記録媒体固有の鍵情報は、

上記第1の送信手段により上記情報処理装置へ送られることを特徴とする信号処理システム。

【請求項13】 請求項12において、

上記第3の鍵情報は、

上記再生装置において前期第1の乱数生成手段により生成された第7の乱数に基づいた鍵情報であるとともに、

当該第3の鍵情報は、

上記第1の送信手段により上記情報処理装置に送られることを特徴とする信号処理システム。

【請求項14】 請求項12において、

上記第3の鍵情報は、

上記情報処理装置において上記第2の乱数生成手段により生成された第8の乱数に基づいた鍵情報であることを特徴とする信号処理システム。

【請求項15】 請求項11において、

上記鍵情報暗号化手段、上記暗号化鍵情報記録手段、上記コンテンツ情報記録手段は、 上記情報処理装置が有しており、

上記記録媒体固有の鍵情報は、

上記第1の送信手段により上記情報処理装置へ送られるとともに、

上記最終暗号化鍵生成手段は、

上記再生装置が有しており、

上記最終暗号化鍵生成手段により生成された上記コンテンツ情報暗号化鍵は、

上記第1の送信手段により上記情報処理装置へ送られることを特徴とする信号処理システム。

【請求項16】 請求項15において、

上記第3の鍵情報は、

上記再生装置において上記第1の乱数生成手段により生成された第9の乱数を基にした鍵情報であることを特徴とする請求項13に記載の信号処理システム。

【請求項17】 請求項15において、

上記第3の鍵情報は、

上記情報処理装置において上記第2の乱数生成手段により生成された第10の乱数を基にした鍵情報であるとともに、

上記伝達手段を介して、上記共通鍵を用いた共通鍵暗号方式で上記情報処理装置から上記再生装置へ情報を送る第2の送信手段により上記再生装置の上記最終暗号化鍵生成手段に送られることを特徴とする信号処理システム。

【請求項18】 請求項10において、

上記記録媒体から読み出される暗号化された第4の鍵情報を、少なくとも上記記録媒体固有の鍵情報を用いて復号する鍵情報復号手段と、

上記第4の鍵情報に基づいてコンテンツ情報復号鍵を生成する最終復号鍵生成手段と、 上記コンテンツ情報復号鍵を用いて上記コンテンツ情報を復号するコンテンツ情報復号手段とを備えていることを特徴とする信号処理システム。

【請求項 19】 請求項 18 において、
上記最終復号鍵生成手段、上記コンテンツ情報復号手段は、
上記情報処理装置が有していることを特徴とする信号処理システム。

【請求項 20】 請求項 19 において、
上記鍵情報復号手段は、
上記情報処理装置が有しており、
上記記録媒体固有の鍵情報は、
上記第 1 の送信手段によって上記情報処理装置へ送られることを特徴とする信号処理システム。

【請求項 21】 請求項 19 において、
上記鍵情報復号手段は、
上記再生装置が有しており、
復号された上記第 4 の鍵情報は、
上記第 1 の送信手段によって上記情報処理装置へ送られることを特徴とする信号処理システム。

【請求項 22】 請求項 18 において、
上記最終復号鍵生成手段は、
上記再生装置が有していることを特徴とする信号処理システム。

【請求項 23】 請求項 22 において、
上記鍵情報復号手段は、
上記再生装置が有しており、
上記再生装置において生成された上記コンテンツ情報復号鍵は、
上記第 1 の送信手段によって上記情報処理装置へ送られることを特徴とする信号処理システム。

【請求項 24】 不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有し、上記コンテンツ情報が伝達手段を介して情報処理装置に送信され、処理される信号処理システムにおける再生装置であって、

当該再生装置を表す情報と上記リボケーション情報とを用いて当該再生装置を

無効化すべきか否かを判定する第1の判定手段を有し、

上記第1の判定手段によって無効化すべきという判定をされなかった場合に生成される第1の鍵情報と、

上記情報処理装置に設けられている当該情報処理装置を表す情報と上記リボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第2の判定手段によって無効化すべきという判定をされなかった場合に生成される第2の鍵情報とを用いて、上記情報処理装置と相互に認証する相互認証手段と、

上記相互認証手段による相互認証後に、上記情報処理装置と共通の共通鍵を生成する共通鍵生成手段とを備えることを特徴とする再生装置。

【請求項25】 不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、再生装置がコンテンツ情報を読み出し、上記コンテンツ情報が伝達手段を介して受信され、処理される情報処理装置であって、

上記再生装置に設けられている第1の判定手段によって、当該再生装置を表す情報と上記リボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定し、上記第1の判定手段によって無効化すべきという判定をされなかった場合に生成される第1の鍵情報と、

当該情報処理装置を表す情報と上記リボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第2の判定手段を有し、

上記第1の鍵情報と、上記第2の判定手段によって無効化すべきという判定をされなかった場合に生成される第2の鍵情報とを用いて、上記再生装置と相互に認証する相互認証手段と、

上記相互認証手段による相互認証後に、上記再生装置と共通の共通鍵を生成する共通鍵生成手段とを備えることを特徴とする情報処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、例えばパーソナルコンピュータと接続されたドライブによってディスクメディアに暗号化コンテンツを記録し、また、ディスクメディアから暗号

化コンテンツを再生する場合に適用される相互認証方法、プログラム、記録媒体、信号処理システム、再生装置および情報処理装置に関する。

【0002】

【従来の技術】

近年開発されたDVD (Digital Versatile Disc またはDigital Video Disc) 等の記録媒体では、1枚の媒体に例えば映画1本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となってくると不正コピーを防止して著作権の保護を図ることがますます重要となっている。

【0003】

DVD-Videoでは、コピープロテクション技術としてCSS (Content Scrambling System) が採用されている。CSSは、DVD-ROMメディアに対する適用のみが認可されており、DVD-R、DVD-RW、DVD+R、DVD+RW等の記録型DVDでのCSSの利用がCSS契約によって禁止されている。したがって、CSS方式で著作権保護されたDVD-Videoの内容を記録型DVDへのまるごとコピー（ビットバイビットコピー）することは、CSS契約上では、認められた行為ではない。

【0004】

しかしながら、CSSの暗号方式が破られる事態が発生した。CSSの暗号化を解除してDVD-Videoの内容を簡単にハードディスクにコピーすることを可能とする「DeCSS」と呼ばれるソフトウェアがインターネット上で配布された。「DeCSS」が出現した背景には、本来耐タンパー化が義務付けられているはずのCSS復号用の鍵データを耐タンパー化しないまま設計された再生ソフトウェアがリバースエンジニアされて鍵データが解読されたことによって、連鎖的にCSSアルゴリズム全体が解読された経緯がある。

【0005】

CSSの後に、DVD-Audio等のDVD-ROMの著作権保護技術であるCPPM (Content Protection for Pre-Recorded Media)、並びに記録型DVD、メモ리카ードに関する著作権保護技術CPRM (Content Protection for Record

able Media) が提案されている。これらの方式は、コンテンツの暗号化や管理情報の格納等に問題が生じたときに、システムを更新でき、また、データをまるごとコピーしても再生を制限できる特徴を有している。DVDに関する著作権保護の方法に関しては、下記の非特許文献1に説明され、CPRMは、ライセンス管理者である米4C Entity, LLCが配布する下記の資料（非特許文献2）に説明されている。

【0006】

【非特許文献1】

山田, 「DVDを起点に著作権保護空間を広げる」, 日経エレクトロニクス 2001.8.13, p.143-153

【0007】

【非特許文献2】

"Content Protection for Recordable Media Specification DVD Book", インターネット<URL: <http://www.4Centity.com/>>

【0008】

【発明が解決しようとする課題】

パーソナルコンピュータ（以下、適宜PCと略す）環境下では、PCとドライブとが標準的インターフェースで接続されるために、標準的インターフェースの部分で秘密保持が必要なデータが知られたり、データが改ざんされるおそれがある。また、アプリケーションソフトウェアがリバースエンジニアリングされ、秘密情報が盗まれたり、改ざんされる危険がある。このような危険性は、記録再生装置が一体に構成された電子機器の場合では、生じることが少ない。

【0009】

著作権保護技術をPC上で実行されるアプリケーションプログラムへ実装する際には、その著作権保護技術の解析を防ぐため耐タンパー性を持たせるのが一般的である。しかしながら、耐タンパー性の強度を示す指標がなく、その結果、どの程度のリバースエンジニアリングへの対応を行うかは、インプレメンターの個々の判断や能力に委ねられているのが現状である。CSSの場合は、結果としてその著作権保護技術が破られてしまった。さらに、CSSの後に提案されたCP

P Mおよび記録型DVDに関する著作権保護技術C P R Mにおいても、既に破られているC S Sに新たな機能を加えたものであり、また、著作権保護技術に関わるアルゴリズムは、大部分がP Cでの実装に依存するものであり、コンテンツプロテクションの機能が十分に強いものと言えない問題があった。すなわち、アプリケーションソフトウェアなどのリバースエンジニアリングによって、著作権保護技術に関わる秘密情報の解析により暗号方式が破られ、ディスクからのデータとしてP Cがそのまま読み出した暗号化コンテンツが「D e C S S」のような解読ソフトウェアにより復号され、平文のままのクリア・コンテンツとしてコピー制限の働かない状態で複製が繰り返されるような事態を招くことで、著作権保護が機能しなくなるという危険性があった。

【0010】

したがって、この発明の目的は、P C環境下でも著作権保護技術の安全性を確保することができる相互認証方法、プログラム、記録媒体、信号処理システム、再生装置および情報処理装置を提供することにある。

【0011】

【課題を解決するための手段】

上述した課題を解決するために、請求項1の発明は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、再生装置がコンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法において、

再生装置は、当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第1の判定ステップを有し、

情報処理装置は、当該情報処理装置を表す情報とリボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第2の判定ステップを有し、

第1の判定手段によって無効化すべきという判定をされなかった場合に生成される第1の鍵情報と、第2の判定手段によって無効化すべきという判定をされなかった場合に生成される第2の鍵情報とを用いて、再生装置と情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法であ

る。

【0012】

請求項4の発明は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、再生装置がコンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法のプログラムであって、

再生装置は、当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第1の判定ステップを有し、

情報処理装置は、当該情報処理装置を表す情報とリボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第2の判定ステップを有し、

第1の判定手段によって無効化すべきという判定をされなかった場合に生成される第1の鍵情報と、第2の判定手段によって無効化すべきという判定をされなかった場合に生成される第2の鍵情報とを用いて、再生装置と情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法のプログラムである。

【0013】

請求項5の発明は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、再生装置がコンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置と相互に認証する相互認証方法のプログラムを格納した記録媒体であって、

再生装置は、当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第1の判定ステップを有し、

情報処理装置は、当該情報処理装置を表す情報とリボケーション情報を用いて当該情報処理装置を無効化すべきか否かを判定する第2の判定ステップを有し、

第1の判定手段によって無効化すべきという判定をされなかった場合に生成される第1の鍵情報と、第2の判定手段によって無効化すべきという判定をされなかった場合に生成される第2の鍵情報とを用いて、再生装置と情報処理装置とが相互に認証する相互認証ステップとを有することを特徴とする相互認証方法のプ

プログラムを格納した記録媒体である。

【0014】

請求項6の発明は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有する再生装置と、再生装置がコンテンツ情報を伝達手段を介して送受信し、処理する情報処理装置とを備える信号処理システムであって、

再生装置は、当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第1の判定手段を有し、

情報処理装置は、当該情報処理装置を表す情報とリボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第2の判定手段を有し、

第1の判定手段によって無効化すべきという判定をされなかった場合に生成される第1の鍵情報と、第2の判定手段によって無効化すべきという判定をされなかった場合に生成される第2の鍵情報とを用いて、再生装置と情報処理装置とが相互に認証する相互認証手段と、

相互認証手段による相互認証後に、再生装置および情報処理装置に共通の共通鍵を生成する共通鍵生成手段とを備えることを特徴とする信号処理システムである。

【0015】

請求項24の発明は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、コンテンツ情報を読み出す再生部を有し、コンテンツ情報が伝達手段を介して情報処理装置に送信され、処理される信号処理システムにおける再生装置であって、

当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定する第1の判定手段を有し、

第1の判定手段によって無効化すべきという判定をされなかった場合に生成される第1の鍵情報と、

情報処理装置に設けられている当該情報処理装置を表す情報とリボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第2の判定手段によって無効化すべきという判定をされなかった場合に生成される第2の鍵情

報とを用いて、情報処理装置と相互に認証する相互認証手段と、

相互認証手段による相互認証後に、情報処理装置と共通の共通鍵を生成する共通鍵生成手段とを備えることを特徴とする再生装置である。

【0016】

請求項 25 の発明は、不正な電子機器を判別するためのリボケーション情報と記録媒体固有の情報とを予め備えた記録媒体から、再生装置がコンテンツ情報を読み出し、コンテンツ情報が伝達手段を介して受信され、処理される情報処理装置であって、

再生装置に設けられている第 1 の判定手段によって、当該再生装置を表す情報とリボケーション情報とを用いて当該再生装置を無効化すべきか否かを判定し、第 1 の判定手段によって無効化すべきという判定をされなかった場合に生成される第 1 の鍵情報と、

当該情報処理装置を表す情報とリボケーション情報とを用いて当該情報処理装置を無効化すべきか否かを判定する第 2 の判定手段を有し、

第 1 の鍵情報と、第 2 の判定手段によって無効化すべきという判定をされなかった場合に生成される第 2 の鍵情報とを用いて、再生装置と相互に認証する相互認証手段と、

相互認証手段による相互認証後に、再生装置と共通の共通鍵を生成する共通鍵生成手段とを備えることを特徴とする情報処理装置である。

【0017】

この発明では、メディア上に記録された鍵情報 (MKB) と各デバイスまたは各アプリケーションに記憶されている鍵情報 (デバイスキー) から同一の値として導かれる鍵情報 (メディアキー) を利用して相互認証がなされる。したがって、この発明においては、認証のためだけに用意される特定の認証鍵を必要とせず、秘密情報を少なくでき、また、デバイスまたはアプリケーションによってデバイスキーを異ならせることが可能であるので、秘密情報が不正に読み取られる危険性を少なくできる。また、この発明では、著作権保護技術に関する秘密情報である電子機器またはアプリケーションソフトウェア固有の情報例えばデバイスキーがドライブ内に実装されているので、情報処理装置にインストールされるアプ

リケーションソフトウェアは、著作権保護技術に関する秘密情報の全てを持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

【0018】

また、電子機器固有の情報としてのデバイスキーを記録再生装置が持つことによって、記録再生装置自身をリボークすることが可能となる。さらに、この発明では、情報処理装置におけるコンテンツキーを計算するのに必要とされる乱数情報が記録再生装置内の例えばLSIによって生成できるので、PC内でソフトウェアによって乱数を生成するのと比較して、真正または真正乱数に近い乱数を生成することができる。したがって、乱数が固定値に置き換えられる、等のおそれを少なくできる。

【0019】

【発明の実施の形態】

この発明の一実施形態の説明に先立って、本明細書の特許請求の範囲において使用される用語と実施の形態中で使用される用語との対応関係について以下に説明する。

【0020】

記録媒体：メディア例えばディスク、再生装置：ドライブ、情報処理装置：ホスト、伝達手段：ドライバ－ホストインターフェース、信号処理システム：メディアを再生するドライブとホストとがドライバ－ホストインターフェースを介して接続されるシステムである。第1の送信手段：ドライブ側からセッションキーを共通鍵とした共通鍵暗号方式で情報をホスト側にする手段、第2の送信手段：逆にホスト側からセッションキーを共通鍵として情報をドライブ側にする手段のことである。

【0021】

コンテンツ情報：メディアに記録されている情報または記録すべき情報をコンテンツ情報としている。リボケーション情報：メディアに予め記録されているメディアキーブロックMKB(Media Key Blocks)、記録媒体固有の情報：メディア

I D、デバイスキー：再生装置または情報処理装置を表す情報、装置を無効化すべきか否かを判定する判定手段：プロセスMKBである。プロセスMKBでは、ドライブ側の第1の判定手段によりドライブが無効化されなければ、ドライブ側のメディアキーとして第1の鍵情報が生成され、ホスト側の第2の判定手段によりホストが無効化されなければ、ホスト側のメディアキーとして第2の鍵情報が生成される。ドライブとホストは、独立して無効化が可能であり、無効化された場合は、期待されるメディアキーを得ることができないので「第1の」、「第2の」と分けている。

【0022】

相互認証手段：A K E (Authentication and Key Exchange) (プロセスMKB以降の乱数交換、M A C 計算、比較からなるドライブ側の第1の確認手段とホスト側の第2の確認手段により相互に相手の動作を確認することである。ドライブ側とホスト側の何れが先に確認するかの順番は、任意であるので、用語の統一を図るために、ドライブ側の確認手段を「第1の」としている。)

【0023】

共通鍵：セッションキー (確実に暗号化・復号に使われるセッションキーとコンテンツキーとは、「鍵」でそれ以外は「鍵情報」としている。認証完了後なので共通鍵として同じ暗号化鍵が生成されるが、生成している装置と、基にしている鍵情報の呼び方を変えていることから、ドライブ側の生成手段を第1の共通鍵生成手段、ホスト側の生成手段を第2の共通鍵生成手段としている。)

【0024】

乱数を生成する乱数生成手段：乱数発生器 (R N G : Random Number Generator) (ドライブ側の乱数生成手段を第1の乱数生成手段、ホスト側の乱数生成手段を第2の乱数生成手段とし、特許請求の範囲においては、生成される乱数に対して請求項に出てくる順番で番号をつけている。)

【0025】

所定の計算を行う計算手段：M A C (Message Authentication Code) 演算ブロック (乱数交換手段により交換された乱数を用いて、ドライブ側で計算する手段を第1の計算手段、ホスト側の計算手段を第2の計算手段としている。)

【0026】

比較手段：比較（ドライブ側の比較を第1の比較手段、ホスト側の比較を第2の比較手段としている。）

【0027】

記録媒体固有の鍵情報：メディアユニークキー（本実施形態においては、メディアユニークキーの生成は耐タンパー性を持たせるために全てドライブ側で行われているので、記録媒体固有の鍵情報（メディアユニークキー）を生成する中間鍵生成手段は、ドライブ側のみとしている。）

【0028】

コンテンツ情報暗号化鍵またはコンテンツ情報復号鍵の基になる鍵情報：（記録時に使われるタイトルキーを第3の鍵情報、再生時に使われるタイトルキーを第4の鍵情報としている。また、メディアユニークキーによってタイトルキーを暗号化する手段を鍵情報暗号化手段、復号する手段を鍵情報復号手段としている。メディアユニークキーによって暗号化されたタイトルキーを記録媒体に記録する手段を暗号化鍵情報記録手段としている。）

【0029】

コンテンツ情報を暗号化または復号するための鍵：コンテンツキー（記録時に使われるコンテンツキーをコンテンツ情報暗号化鍵とし、再生時に使われるコンテンツキーをコンテンツ情報復号鍵としている。コンテンツ情報暗号化鍵を生成する手段を最終暗号化鍵生成手段、コンテンツ情報復号鍵を生成する手段を最終復号鍵生成手段としている。暗号化されたコンテンツ情報を記録媒体に記録する手段をコンテンツ情報記録手段とし、暗号化されたコンテンツ情報を復号する手段をコンテンツ情報復号手段としている。）

【0030】

次に、この発明の理解の容易のために、最初に図1を参照して著作権保護技術例えばDVD用CPRMのアーキテクチャについて説明する。図1において、参照符号1が例えばCPRM規格に準拠したDVD-R/RW、DVD-RAM等の記録型DVDメディアを示し、参照符号2が例えばCPRM規格に準拠したレコーダを示し、参照符号3が例えばCPRM規格に準拠したプレーヤを示す。レ

コーダ2およびプレーヤ3は、機器またはアプリケーションソフトウェアである。

【0031】

未記録ディスクの状態において、DVDメディア1の最内周側のリードインエリアのBCA (Burst Cutting Area) またはNBCA (Narrow Burst Cutting Area) と称されるエリアには、メディアID11が記録され、リードインエリアのエンボスまたはプリ記録データゾーンには、メディアキーブロック（以下、MKBと適宜略す）12が予め記録されている。メディアID11は、個々のメディア単位例えばディスク1枚毎に異なる番号であり、メディアの製造者コードとシリアル番号から構成される。メディアID11は、メディアキーを個々のメディアで異なるメディアユニークキーへ変換する際に必要となる。メディアキーブロックMKBは、メディアキーの導出、並びに機器のリボケーション（無効化）を実現するための鍵束である。これらのメディアIDおよびメディアキーブロックは、記録媒体固有の第1の情報である。

【0032】

ディスク1の書き換えまたは追記可能なデータ領域には、コンテンツキーで暗号化された暗号化コンテンツ13が記録される。暗号化方式としては、C2 (Cryptomeria Cipherng) が使用される。

【0033】

DVDメディア1には、暗号化タイトルキー14およびCCI (Copy Control Information) 15が記録される。暗号化タイトルキー14は、暗号化されたタイトルキー情報であり、タイトルキー情報は、タイトル毎に付加される鍵情報である。CCIは、コピーノーマ、コピーワンス、コピーフリー等のコピー制御情報である。

【0034】

レコーダ2は、デバイスキー21、プロセスMKB22、C2__G23、乱数発生器24、C2__E25、C2__G26およびC2__ECBC27の構成要素を有する。プレーヤ3は、デバイスキー31、プロセスMKB32、C2__G33、C2__D35、C2__G36およびC2__DCBC37の構成要素を有する。

【0035】

デバイスキー 21、31 は、個々の装置メーカ、またはアプリケーションソフトウェアベンダー毎に発行された識別番号である。デバイスキーは、ライセンス管理者によって正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の情報である。DVDメディア 1 から再生された MKB 12 とデバイスキー 21 とがプロセス MKB 22 において演算されることによって、リボケーションされたかどうかの判別ができる。レコーダ 2 におけるのと同様に、プレーヤ 3 においても、MKB 12 とデバイスキー 31 とがプロセス MKB 32 において演算され、リボケーションされたかどうかの判別がなされる。

【0036】

さらに、プロセス MKB 22、32 のそれぞれにおいて、MKB 12 とデバイスキー 21、31 からメディアキーが算出される。MKB 12 の中にレコーダ 2 またはプレーヤ 3 のデバイスキーが入っておらず、演算された結果が予め決められたある値例えばゼロの値と一致した場合、そのデバイスキーを持つレコーダ 2 またはプレーヤ 3 が正当なものでないと判断される。すなわち、そのようなレコーダ 2 またはプレーヤ 3 がリボケーションされる。

【0037】

C2__G23、33 は、それぞれ、メディアキーとメディア ID とを演算し、メディアユニークキーを導出する処理である。

【0038】

乱数発生器 (RNG: Random Number Generator) 24 は、タイトルキーの生成に利用される。乱数発生器 24 からのタイトルキーが C2__E25 に入力され、タイトルキーがメディアユニークキーで暗号化される。暗号化タイトルキー 14 が DVD メディア 1 に記録される。

【0039】

プレーヤ 3 では、DVD メディア 1 から再生された暗号化タイトルキー 14 とメディアユニークキーとが C2__D35 に供給され、暗号化タイトルキーがメデ

ィアユニークキーで復号され、タイトルキーが得られる。

【0040】

レコーダ2においては、CCIとタイトルキーとがC2__G26に供給され、コンテンツキーが導出される。コンテンツキーがC2__ECBC27に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ13がDVDメディア1に記録される。

【0041】

プレーヤ3においては、CCIとタイトルキーとがC2__G36に供給され、コンテンツキーが導出される。コンテンツキーがC2__ECBC37に供給され、DVDメディア1から再生された暗号化コンテンツ13がコンテンツキーを鍵として復号される。

【0042】

図1の構成において、レコーダ2による記録の手順について説明する。レコーダ2は、DVDメディア1からMKB12を読み出し、プロセスMKB22によってデバイスキー21とMKB12とを演算し、メディアキーを計算する。演算結果が予め定められた値を示すならば、デバイスキー21（レコーダ2の機器またはアプリケーション）がMKBによってリボークされたと判定され、レコーダ2は、以後の処理を中断し、DVDメディア1への記録を禁止する。若し、メディアキーの値が予め定められた値以外であれば、処理を継続する。

【0043】

次に、レコーダ2は、DVDメディア1からメディアID11を読み、メディアキーと共にメディアIDをC2__G23に入力しメディア毎に異なるメディアユニークキーが演算される。乱数発生器24で発生させたタイトルキーがC2__E25で暗号化され、暗号化タイトルキー14としてDVDメディア1に記録される。また、タイトルキーとコンテンツのCCI情報がC2__G26で演算され、コンテンツキーが導出される。コンテンツキーでコンテンツをC2__ECBC27で暗号化し、DVDメディア1上に暗号化コンテンツ13としてCCI15と共に記録する。

【0044】

プレーヤ 3 による再生の手順について説明する。最初に MKB 12 を DVD メディア 1 から読み出し、デバイスキー 31 と MKB 12 を演算し、リボケーションの確認がなされる。デバイスキー 31、すなわち、プレーヤ 3 の機器またはアプリケーションがリボークされない場合には、メディア ID を使用してメディアユニークキーが演算され、読み出された暗号化タイトルキー 14 とメディアユニークキーからタイトルキーが演算される。タイトルキーと CCI 15 とが C2__G36 に入力され、コンテンツキーが導出される。コンテンツキーが C2__DCBC37 に入力され、コンテンツキーを鍵として、DVD メディア 1 から再生された暗号化コンテンツ 13 に対して C2__DCBC37 の演算が施される。その結果、暗号化コンテンツ 13 が復号される。

【0045】

このように、コンテンツの復号に必要なコンテンツキーを得るためには、DVD メディアの 1 枚毎に異なるメディア ID が必要となるので、たとえメディア上の暗号化コンテンツが忠実に他のメディアにコピーされても、他のメディアのメディア ID がオリジナルのメディア ID と異なるために、コピーされたコンテンツを復号することができず、コンテンツの著作権を保護することができる。

【0046】

上述した図 1 の構成は、記録再生機器として構成されたものである。この発明は、DVD メディア 1 に対するコンテンツ保護処理を PC 環境下で扱う場合に適用される。図 2 を参照して現行の方式による PC とドライブの役割分担を示す。図 2 において、参照符号 4 が上述した CPRM 規格に準拠した DVD メディア 1 を記録および再生する記録再生装置としての DVD ドライブを示す。

【0047】

参照符号 5 がデータ処理装置としてのホスト例えば PC を示す。ホスト 5 は、DVD メディア 1 に記録可能で、DVD メディア 1 から再生可能なコンテンツを扱うことができ、且つ DVD ドライブ 4 と接続されてデータ交換が可能な装置またはアプリケーションソフトウェアである。例えば PC に対してアプリケーションソフトウェアがインストールされることによってホスト 5 が構成される。

【0048】

DVDドライブ4とホスト5との間がインターフェース4aで接続されている。インターフェース4aは、ATAPI(AT Attachment with Packet Interface), SCSI(Small Computer System Interface), USB(Universal Serial Bus), IEEE(Institute of Electrical and Electronics Engineers)1394等である。

【0049】

DVDメディア1には、メディアID11、メディアキープブロック12およびACC(Authentication Control Code)が予め記録されている。ACCは、DVDドライブ4とホスト5との間の認証がDVDメディア1によって異なるようにするために予めDVDメディア1に記録されたデータである。

【0050】

DVDドライブ4は、ACC16をDVDメディア1から読み出す。DVDメディア1から読み出されたACC16がDVDドライブ4のAKE(Authentication and Key Exchange)41に入力されると共に、ホスト5へ転送される。ホスト5は、受け取ったACCをAKE51に入力する。AKE41および51は、乱数データを交換し、この交換した乱数とACCの値とから認証動作の度に異なる値となる共通のセッションキー(バスキーと称する)を生成する。

【0051】

バスキーがMAC(Message Authentication Code)演算ブロック42および52にそれぞれ供給される。MAC演算ブロック42および52は、AKE41および51でそれぞれ得られたバスキーをパラメータとして、メディアIDおよびメディアキープブロック12のMACを計算するプロセスである。MKBとメディアIDの完全性(integrity)をホスト5が確認するために利用される。

【0052】

MAC42および52によってそれぞれ計算されたMACがホスト5の比較53において比較され、両者の値が一致するかどうか判定される。これらのMACの値が一致すれば、MKBとメディアIDの完全性が確認されたことになる。比較出力でスイッチSW1が制御される。

【0053】

スイッチSW1は、DVDドライブ4のDVDメディア1の記録または再生経路と、ホスト5の暗号化／（または）復号モジュール54との間の信号路をON／OFFするものとして示されている。なお、スイッチSW1は、信号路のON／OFFを行うものとして示されているが、より実際には、ONの場合にホスト5の処理が継続し、OFFの場合にホスト5の処理が停止することを表している。暗号化／復号モジュール54は、メディアユニークキーと暗号化タイトルキーとCCIとからコンテンツキーを算出し、コンテンツキーを鍵としてコンテンツを暗号化コンテンツ13へ暗号化し、またはコンテンツキーを鍵として暗号化コンテンツ13を復号する演算ブロックである。

【0054】

メディアユニークキー演算ブロック55は、MKB12とメディアIDとデバイスキー56とからメディアユニークキーを演算する演算ブロックである。すなわち、図1に示すレコーダまたはプレーヤと同様に、デバイスキーとMKB12とからメディアキーが演算され、さらに、メディアキーとメディアID11とからメディアユニークキーが演算される。メディアキーが所定の値となった場合には、その電子機器またはアプリケーションソフトウェアが正当なものではないと判断され、リボークされる。したがって、メディアユニークキー演算ブロック55は、リボケーションを行うリボーク処理部としての機能も有する。

【0055】

記録時に、比較53によって完全性が確認された場合には、スイッチSW1がONされ、暗号化／復号モジュール54からスイッチSW1を通じてドライブ4に対して、暗号化コンテンツ13、暗号化タイトルキー14およびCCI15が供給され、DVDメディア1に対してそれぞれ記録される。再生時に、比較53によって完全性が確認された場合には、スイッチSW1がONされ、DVDメディア1からそれぞれ再生された暗号化コンテンツ13、暗号化タイトルキー14およびCCI15がスイッチSW1を通じてホスト5の暗号化／復号モジュール54に対して供給され、暗号化コンテンツが復号される。

【0056】

図3は、図2に示す現行のPC環境下のDVDメディアを利用するシステムに

において、DVDメディア1と、DVDドライブ4と、ホスト5との間の信号の授受の手順を示す。ホスト5がDVDドライブ4に対してコマンドを送り、DVDドライブ4がコマンドに応答した動作を行う。

【0057】

最初に、ホスト5からの要求に応じてDVDメディア1上のACCがシークされ、読み出される（ステップS1）。次のステップS2において、読み出されたACCがAKE41に入力されると共に、ホスト5へ転送され、ホスト5では、受け取ったACCがAKE51へ入力される。AKE41および51は、乱数データを交換し、この交換した乱数とACC16の値から認証動作の度に異なる値となるセッションキーとしてのバスキーを生成し、バスキーをDVDドライブ4とホスト5が共有する。相互認証が成立しなかった場合では、処理が中断する。

【0058】

認証動作は、電源のON後のディスク検出時並びにディスクの交換時には、必ず行われる。また、記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行うようにしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

【0059】

認証が成功すると、次に、ステップS3において、ホスト5がDVDドライブ4に対して、DVDメディア1からのMKB（メディアキーブロック）パック#0の読み出しを要求する。MKBは、パック0～パック15の16セクタが12回繰り返してリードインエリアに記録されている。パック単位で、エラー訂正符号化がなされている。

【0060】

DVDドライブ4がステップS4においてMKBのパック#0を読みに行き、ステップS5において、パック#0が読み出される。DVDドライブ4は、モディファイドMKBをホスト5へ戻す（ステップS6）。すなわち、MKBを読み出す際に、バスキーをパラメータとしてMAC値を計算し、MKBに対してMAC値を付加してホスト5へデータを転送する。パック#0以外の残りのMKBパックの要求と、DVDドライブ4の読み出し動作と、モディファイドMKBパッ

クの転送動作とがMKBのバックがなくなるまで、例えばバック#15が読み出され、ホスト5へ転送されるまで、ステップS7およびS8によって繰り返される。

【0061】

次に、ホスト5がDVDドライブ4に対してメディアIDを要求する。DVDドライブ4がDVDメディア1に記録されているメディアIDを読みに行き、ステップS11において、メディアIDが読み出される。DVDドライブ4は、メディアIDを読み出す際に、バスキーをパラメータとしてそのMAC値を計算し、ステップS12において、読み出されたメディアIDに対してMAC値m1を付加してホスト5へデータを転送する。

【0062】

ホスト5では、DVDドライブ4から受け取ったMKB12およびメディアID11からバスキーをパラメータとして再度MAC値を計算し、計算したMAC値とDVDドライブ4から受け取ったMAC値とを比較53で比較し、両者が一致したならば、正しいMKBおよびメディアIDを受け取ったと判定して、スイッチSW1をONに設定して処理を先に進める。逆に両者が一致しなかったならば、MKBおよびメディアIDが改ざんされたものと判定して、スイッチSW1をOFFに設定して処理を中断する。

【0063】

ステップS13において、ホスト5がDVDドライブ4に対して暗号化コンテンツを要求し、ステップS14において、DVDドライブ4が暗号化コンテンツを読み出し、ステップS13において、読み出した暗号化コンテンツがホスト5に転送される。ホスト5のメディアユニークキー演算ブロック55では、デバイスキー56とMKB12とメディアID11とによってメディアユニークキーが計算される。そして、メディアユニークキーが暗号化／復号モジュール54に供給され、暗号化タイトルキー14、CCI15からコンテンツキーが求められ、コンテンツキーを鍵としてDVDメディア1から読み出された暗号化コンテンツが復号され、また、DVDメディア1に対して記録されるコンテンツが暗号化される。

【0064】

図4のフローチャートにおいて、ステップST1は、MAC演算ブロック42でバスキーをパラメータとして求められたMAC計算値と、MAC演算ブロック53でバスキーをパラメータとして求められたMAC計算値とを比較するステップである。両者が一致すれば、スイッチSW1がステップST2においてONとされ、両者が一致しない場合では、スイッチSW1がステップST3においてOFFとされ、処理が停止する。

【0065】

上述したCPRMでは、DVD-Videoの著作権保護技術であるCSSと同じバスキー生成方法を採用している。CSS認証方式の内容は、本来秘密であるべき情報であるが、既に解析され一般ユーザーが入手可能なCSSライセンス管理団体であるDVD-CCAの許諾を得ていないフリーソフトウェアによって動作させることが可能となっている。また、コンテンツプロテクション処理は、ホスト側でなされる、すなわち、リボケーション判定、メディアキー取得、メディアユニークキー導出、タイトルキー生成・導出からコンテンツキー導出およびコンテンツ暗号化・復号の全てがホスト側の処理であることから、著作権保護技術としての信頼性が低下している。

【0066】

以下に述べるこの発明は、かかる問題点を解決するものである。一実施形態では、PC環境下でのコンテンツプロテクション処理におけるPCとドライブの役割分担におけるリボケーション動作とメディアキー導出に関わる情報（ここでは、デバイスキー）をドライブ内部に持ち、PCとの相互認証を経てセッションキーを導出するものである。

【0067】

図5は、一実施形態における相互認証の構成を示すブロック図であり、図6は、ドライブ側の処理の流れを示すフローチャートであり、図7は、ホスト側の処理の流れを示すフローチャートである。以下の説明において、参照符号101がメディア例えば光ディスクを示し、参照符号102がメディアのドライブを示し、参照符号103がドライブ102とドライバーストインターフェース104

を介して接続されたホストを示す。メディア101は、上述したDVDメディアと同様の情報が予め記録されているものである。メディア101は、記録可能なものに限らず、読み出し専用のものでも良い。ホスト103がドライブ102に対して所定のコマンドを送り、その動作を制御する。使用するコマンドは、上述した非特許文献2に記載されているコマンド並びにコマンドを拡張したもの、および、メディア101からコンテンツをセクタ・データとして読み出すためのREADコマンド、メディア101へコンテンツをセクタ・データとして書き込むためのWRITEコマンドである。

【0068】

ドライブ102は、ドライブのデバイスキー121を有し、ホスト103がホストのデバイスキー131を有している。デバイスキー121は、多くの場合にLSI (Large Scale Integrated Circuit: 大規模集積回路) 内部に配置され、外部から読み出すことができないようセキュアに記憶される。デバイスキー131は、ソフトウェアプログラム内にセキュアに記憶される場合と、ハードウェアとしてセキュアに記憶される場合とがある。また、ドライブ102がメディア101を扱う正当なドライブとなるためには、一実施形態のように、デバイスキーのような著作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりすますようなクローン・ドライブの作成を防止できる効果がある。

【0069】

図5に示すように、ドライブ102には、MKBとデバイスキー121とが入力され、ドライブのデバイスキーがリボケーションされたかどうかを判定するプロセスMKB122が備えられている。ホスト103にも同様に、プロセスMKB132が備えられている。リボケーションされない場合に、プロセスMKB122および132からそれぞれメディアキーKmが出力される。リボーク判定処理がなされ、メディアキーKmが得られてから認証処理がなされる。

【0070】

参照符号123、124および125は、メディアキーKmをパラメータとしてMAC値を計算するMAC演算ブロックをそれぞれ示す。また、参照符号12

6、127および128は、乱数発生器（RNG:Random Number Generator）をそれぞれ示す。乱数発生器126が乱数Ra1を生成し、乱数発生器127が乱数Ra2を生成し、乱数発生器128が乱数Ra3を生成する。乱数発生器126、127、128は、例えばLSIの構成の乱数発生器であり、ソフトウェアにより乱数を発生する方法と比較してより真正乱数に近い乱数を発生することができる。乱数発生器を共通のハードウェアとしても良いが、乱数Ra1、Ra2、Ra3は、互いに独立したものである。

【0071】

ホスト103に、メディアキーKmをパラメータとしてMAC値を計算するMAC演算ブロック133、134および135と、乱数発生器136、137および138が備えられている。乱数発生器136が乱数Rb1を生成し、乱数発生器137が乱数Rb2を生成し、乱数発生器138が乱数Rb3を生成する。乱数発生器136、137、138は、通常はソフトウェアによって乱数を発生するものであるが、ハードウェアによる乱数が利用できる場合にはこれを用いても良い。

【0072】

ドライブ102において生成された乱数とホスト103において生成された乱数とが交換される。すなわち、乱数Ra1および乱数Rb1がMAC演算ブロック123および133に入力され、乱数Ra2および乱数Rb2がMAC演算ブロック124および134に入力され、乱数Ra3および乱数Rb3がMAC演算ブロック125および135に入力される。

【0073】

ドライブ102のMAC演算ブロック123が演算したMAC値と、ホスト103のMAC演算ブロック133が演算したMAC値とがホスト103内の比較139において比較され、二つの値が同一か否かが判定される。ここでのMAC値は、 $e_{Km}(Ra1 \parallel Rb1)$ と表記される。 $e_{Km}()$ は、メディアキーKmを鍵として括弧内のデータを暗号化することを表している。 $Ra1 \parallel Rb1$ の記号は、左側に乱数Ra1を配し、右側に乱数Rb1を配するように、二つの乱数を結合することを表している。比較の結果、二つの値が同一と判定されると、ホスト103による

ドライブ102の認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

【0074】

ホスト103のMAC演算ブロック134が演算したMAC値と、ドライブ102のMAC演算ブロック124が演算したMAC値とがドライブ102内の比較129において比較され、二つの値が同一か否かが判定される。ここでのMAC値は、 $eKm(Rb2 \parallel Ra2)$ と表記される。比較の結果、二つの値が同一と判定されると、ドライブ102によるホスト103の認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

【0075】

かかる相互認証において、比較139および129の両者において、MAC値が同一と判定され、ドライブ102およびホスト103の両者の正当性が確認されると、すなわち、相互認証が成功すると、MAC演算ブロック125および135によって、共通のセッションキー $eKm(Ra3 \parallel Rb3)$ がそれぞれ生成される。

【0076】

さらに、上述した相互認証の処理の流れを図6および図7のフローチャートを参照して説明する。最初に、図7のステップST20において、ホスト103がドライブ102に対して、コマンドREPORT KEYを発行し、MKBの転送を要求する。図6のステップST10において、ドライブ102がメディア101からMKB112を読み出して、ホスト103へ転送する。

【0077】

次に、ドライブ102がステップST11において、プロセスMKB122によってメディアキー Km を計算し、ホスト103がステップST21において、プロセスMKB132によってメディアキー Km を計算する。この計算の過程でそれぞれが内蔵するデバイスキー121および131がリボケーションの対象とされているか否かが自分自身によって確認される（図6中のステップST12、図7中のステップST22）。

【0078】

ドライブ102およびホスト103のそれぞれは、リボケーションの対象とさ

れている場合にはリボークされ、処理が終了する。若し、ホスト103がリボケーションの対象とされていないならば、ステップST23において、コマンドSEND KEYにより、ドライブ102に対して乱数発生器136および137でそれぞれ生成された乱数Rb1と乱数Rb2を転送する。若し、ドライブ102がリボケーションの対象とされていないならば、ステップST13において、ドライブ102がホスト103から転送されたこれらの乱数を受け取る。

【0079】

その後、ホスト103は、コマンドREPORT KEYによりドライブ102に対してドライブ102が持つメディアキーKmを鍵としたMACによるレスポンス値と乱数生成器126が発生した乱数Ra1とをホスト103へ転送することを要求する(ステップST24)。このレスポンス値は、 $eKm(Ra1 \parallel Rb1)$ と表記される。 $eKm()$ は、メディアキーKmを暗号鍵として括弧内のデータを暗号化することを表している。 $Ra1 \parallel Rb1$ の記号は、左側に乱数Ra1を配し、右側に乱数Rb1を配するように、二つの乱数を結合することを表している。

【0080】

ホスト103からコマンドREPORT KEYを受け取ったドライブ102は、ステップST14において、MAC演算ブロック123が生成したMAC値 $eKm(Ra1 \parallel Rb1)$ と乱数Ra1をホスト103へ転送する。ステップST25において、ホスト103は、自身のMAC演算ブロック133でMAC値を計算し、比較139においてドライブ102から受け取った値と一致するかの確認を行う。若し、受け取ったMAC値と計算されたMAC値とが一致したのなら、ホスト103によるドライブ102の認証が成功したことになる。ステップST25における比較の結果が同一でない場合には、ホスト103によるドライブ102の認証が失敗したことになる、リジェクト処理がなされる。

【0081】

ホスト103によるドライブ102の認証が成功した場合には、ステップST26において、ホスト103がドライブ102へコマンドREPORT KEYを送付し、ドライブ102の乱数生成器124および125がそれぞれ生成する乱数Ra2と乱数Ra3の転送を要求する。このコマンドに応答して、ステップST15におい

て、ドライブ102は、これらの乱数をホスト103へ転送する。

【0082】

ステップST27において、ホスト103のMAC演算ブロック134は、ドライブ102から受け取った乱数からホスト103が持つメディアキー K_m を鍵としたMACによるレスポンス値 $eK_m(Rb2 \parallel Ra2)$ を計算し、乱数 $Rb3$ とともに、コマンドSEND KEYを用いてドライブ102へ転送する。

【0083】

ステップST16において、ドライブ102は、ホスト103からレスポンス値 $eK_m(Rb2 \parallel Ra2)$ および乱数 $Rb3$ を受け取ると、自身でMAC値を計算し、ステップST17において、比較129によってホスト103から受け取ったMAC値と一致するかの確認を行う。若し、受け取ったMAC値と計算されたMAC値とが一致したのなら、ドライブ102によるホスト103の認証が成功したことになる。この場合には、ステップST18において、MAC演算ブロック125がセッションキー $eK_m(Ra3 \parallel Rb3)$ を生成し、また、ホスト103に対して認証が成功したことを示す情報を送信し、認証処理が完了する。セッションキーは、認証動作の度に異なる値となる。

【0084】

ステップST17における比較の結果が同一でない場合には、ドライブ102によるホスト103の認証が失敗したことになり、ステップST19において、認証が失敗したことを示すエラー情報がホスト103に送信される。

【0085】

ホスト103は、送付したコマンドSEND KEYに対する応答としてドライブ102から認証が成功したか否かを示す情報を受け取り、受け取った情報に基づいてステップST28において、認証完了か否かを判断する。認証が成功したことを示す情報を受け取ることで認証完了と判断し、認証が失敗したことを示す情報を受け取ることで認証が完了しなかったと判断する。認証が完了した場合は、ステップST29において、MAC演算ブロック135がドライブ側と共通のセッションキー $eK_m(Ra3 \parallel Rb3)$ （例えば64ビット長）を生成する。認証が完了しなかった場合には、リジェクト処理がなされる。セッションキー $eK_m(Ra3 \parallel Rb3)$ を以

下の説明では、適宜 K_s と表記する。

【0086】

上述した一実施形態による相互認証は、ドライブ102がリボケーション機能を持つことができ、また、認証専用の特定の認証鍵を必要としない特徴を有している。

【0087】

また、電子機器固有の情報としてのデバイスキーを記録再生装置が持つことによって、記録再生装置自身をリボークすることが可能となる。

【0088】

さらに、ドライブ102が比較129によってホスト103の認証結果を確認することで、ドライブ102がホスト103から正規のライセンスを受けた上で実装されたものであるか否かを判定することが可能となる。

【0089】

次に、上述した相互認証を行うドライブ102とホスト103とを組み合わせで実現したレコーダの一実施形態の構成を図8に示す。一実施形態のレコーダは、ドライブ102がメディアユニークキーを計算し、計算したメディアユニークキーを相互認証によって生成したセッションキー K_s を用いてセキュアにホスト103に転送する。また、ドライブ102がコンテンツキー導出のための乱数データを生成し、生成した乱数データを相互認証によって生成したセッションキー K_s を用いてホスト103へセキュアに転送し、ホスト103が導出したコンテンツキーを用いてコンテンツを暗号化し、暗号化コンテンツをドライブ102へ転送し、ドライブ102が暗号化コンテンツをメディア101へ記録する構成とされている。

【0090】

レコーダを構成するドライブ102は、デバイスキー121、プロセスMKB122、C2__G2141、DES (Data Encryption Standard) エンクリプタ142、乱数発生器143、DESエンクリプタ144の構成要素を有する。

【0091】

メディア101から再生されたMKB112とデバイスキー121とがプロセ

スMKB122において演算されることによって、リボケーションされたかどうかの判別ができる。プロセスMKB122において、MKB112とデバイスキー121からメディアキーが算出される。MKB112の中にドライブ102のデバイスキー121が入っておらず、演算された結果が予め決められたある値例えばゼロの値と一致した場合、そのデバイスキー121を持つドライブ102が正当なものでないと判断され、ドライブ102がリボケーションされる。

【0092】

C2__G141は、メディアキーとメディアID111とを演算し、メディアユニークキーを導出する処理である。メディアユニークキーがDESエンクリプタ142にてセッションキーKsによって暗号化される。暗号化の方式として、例えばDES CBCモードが使用される。DESエンクリプタ142の出力がホスト103のDESデクリプタ151に送信される。

【0093】

乱数発生器143によってタイトルキーが生成される。乱数発生器143からのタイトルキーがDESエンクリプタ144に入力され、タイトルキーがセッションキーで暗号化される。暗号化タイトルキーがホスト103のDESデクリプタ152に送信される。

【0094】

ホスト103において、DESデクリプタ151において、セッションキーKsによってメディアユニークキーが復号される。DESデクリプタ152において、セッションキーKsによってタイトルキーが復号される。メディアユニークキーおよびタイトルキーがC2__E153に供給され、タイトルキーがメディアユニークキーを使用してC2によって暗号化される。暗号化タイトルキー114がメディア101に記録される。

【0095】

ホスト103においては、CCIと復号されたタイトルキーとがC2__G154に供給され、コンテンツキーが導出される。コンテンツキーがC2__ECBC155に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ113がメディア101に記録される。

【0096】

図9は、コンテンツ記録時の手順を示すものである。最初に、ホスト103からの要求に応じてメディア101上のMKBがシークされ、読み出される（ステップS21）。次のステップS22のAKE (Authentication and Key Exchange) において、上述したようなリボーク処理とドライブ102とホスト103の相互認証動作がなされる。

【0097】

相互認証動作は、電源のON後のディスク検出時並びにディスクの交換時には、必ず行われる。また、記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行うようにしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

【0098】

相互認証が成功しないと、リジェクト処理によって例えば処理が中断する。相互認証が成功すると、ドライブ102およびホスト103の両者において、セッションキーK_sが生成され、セッションキーK_sが共有される。

【0099】

次のステップS23において、ホスト103がドライブ102に対してメディアユニークキーを要求する。ドライブ102は、メディア101のメディアIDをシークし（ステップS24）、メディアIDをメディア101から読み出す（ステップS25）。ドライブ102は、メディアキーとメディアIDとを演算することによってメディアユニークキーを生成する。ステップS26において、メディアユニークキーがセッションキーK_sによって暗号化され、暗号化されたメディアユニークキーがホスト103に転送される。

【0100】

次に、ステップS27において、ホスト103がドライブ102に対してタイトルキーを要求する。ステップS28において、ドライブ102がタイトルキーをセッションキーK_sで暗号化し、暗号化したタイトルキーをホスト103に転送する。ホスト103において、セッションキーK_sによって、暗号化されたメディアユニークキーおよび暗号化されたタイトルキーがそれぞれ復号される。

【0101】

そして、タイトルキーがメディアユニークキーによって暗号化され、暗号化タイトルキーが生成される。また、タイトルキーとCCIからコンテンツキーが生成され、コンテンツキーによってコンテンツが暗号化される。ステップS29において、ホスト103からドライブ102に対して、暗号化タイトルキー、暗号化コンテンツおよびCCIが転送される。ステップS30において、ドライブ102によって、これらの暗号化タイトルキー、暗号化コンテンツおよびCCIがメディア101に対して記録される。

【0102】

なお、図8のレコーダの構成においては、ドライブ102において乱数発生器143を使用してタイトルキーを生成している。しかしながら、ホスト103に乱数発生器を設け、この乱数発生器によってタイトルキーを生成するようにしても良い。

【0103】

次に、上述した相互認証を行うドライブ102とホスト103とを組み合わせで実現したプレーヤの一実施形態の構成を図10に示す。一実施形態のプレーヤは、ドライブ102が計算したメディアユニークキーを相互認証によって生成したセッションキーK_sを用いてセキュアにホスト103に転送し、ホスト103が暗号化タイトルキーをメディアユニークキーによって復号し、タイトルキーとCCIとから導出したコンテンツキーを用いてコンテンツを復号する構成とされている。

【0104】

プレーヤを構成するドライブ102は、デバイスキー121、プロセスMKB122、C2__G2141、DESエンクリプタ142の構成要素を有する。メディア101から再生されたMKB112とデバイスキー121とがプロセスMKB122において演算されることによって、リボケーションされたかどうかの判別ができる。プロセスMKB122において、MKB112とデバイスキー121からメディアキーが算出される。

【0105】

C2__G141は、メディアキーとメディアID111とを演算し、メディアユニークキーを導出する処理である。メディアユニークキーがDESエンクリプタ142にてセッションキーKsによって暗号化される。暗号化の方式として、例えばDES CBCモードが使用される。DESエンクリプタ142の出力がホスト103のDESデクリプタ151に送信される。

【0106】

ホスト103において、DESデクリプタ151において、セッションキーKsによってメディアユニークキーが復号される。メディアユニークキーおよび暗号化タイトルキー114がC2__D153に供給され、暗号化タイトルキーがメディアユニークキーを使用して復号される。復号されたタイトルキーとメディア101から再生されたCCIがC2__G154に供給され、コンテンツキーが導出される。メディア101から再生された暗号化コンテンツ113がC2デクリプタ155において、コンテンツキーによって復号され、コンテンツが得られる。

【0107】

図11は、コンテンツ再生時の手順を示すものである。最初に、ホスト103からの要求に応じてメディア101上のMKBがシークされ、読み出される（ステップS41）。MKBがパック毎に読み出される。次のステップS42のAKEにおいて、上述したようなりボーク処理とドライブ102とホスト103の相互認証動作がなされる。

【0108】

相互認証が成功しないと、リジェクト処理によって例えば処理が中断する。相互認証が成功すると、ドライブ102およびホスト103の両者において、セッションキーKsが生成され、セッションキーKsが共有される。

【0109】

次のステップS43において、ホスト103がドライブ102に対してメディアユニークキーを要求する。ドライブ102は、メディア101のメディアIDをシークし（ステップS44）、メディアIDをメディア101から読み出す（ステップS45）。ドライブ102は、メディアキーとメディアIDとを演算す

ることによってメディアユニークキーを生成する。ステップS46において、メディアユニークキーがセッションキーKsによって暗号化され、暗号化されたメディアユニークキーがホスト103に転送される。

【0110】

次に、ステップS47において、ホスト103がドライブ102に対して、暗号化タイトルキー、CCIおよび暗号化コンテンツを要求する。ステップS48において、ドライブ102が暗号化タイトルキー114、CCI115および暗号化コンテンツ113をメディア101からリードする。ステップS49において、ドライブ102が暗号化タイトルキー114、CCI115および暗号化コンテンツ113を読み取る。そして、ステップS50において、ドライブ102が暗号化タイトルキー114、CCI115および暗号化コンテンツ113をホスト103に対して転送する。

【0111】

ホスト103において、タイトルキーが復号され、タイトルキーとCCIとからコンテンツキーが求められ、コンテンツキーを鍵として暗号化コンテンツが復号される。

【0112】

図10に示すプレーヤの構成においては、ホスト103が暗号化タイトルキーを復号するデクリプタC2__D153を備えているが、ドライブ102が暗号化タイトルキーを復号するデクリプタを備えるようにしても良い。この場合、復号されたタイトルキーがホスト103のコンテンツキー生成用のC2__G154に対してセキュアに転送される。または、ドライブ102にコンテンツキー生成装置C2__Gを設け、ドライブ102において復号されたタイトルキーとCCIとからコンテンツキーを生成するようにしても良い。この場合、復号されたコンテンツキーがホスト103のC2__DCBC155へセキュアに転送される。

【0113】

図12は、相互認証を行うドライブ102とホスト103とを組み合わせることで実現したレコーダの他の実施形態の構成を示す。他の実施形態のレコーダは、ドライブ102が計算したメディアユニークキーを相互認証によって生成したセッシ

セッションキーKsを用いてセキュアにホスト103に転送する。また、ドライブ102においてコンテンツキーが生成され、生成されたコンテンツキーがセッションキーKsを用いてホスト103へセキュアに転送され、ホスト103が復号したコンテンツキーを用いてコンテンツを暗号化し、暗号化コンテンツをドライブ102へ転送し、ドライブ102が暗号化コンテンツをメディア101へ記録する構成とされている。すなわち、図8に示す上述したレコーダでは、ホスト103においてコンテンツキーを生成したが、他の実施形態では、ドライブ102において、コンテンツキーを生成している。

【0114】

図12に示すように、メディア101から再生されたMKB112とデバイスキー121とがプロセスMKB122において演算されることによって、メディアキーが算出され、C2__G141において、メディアキーとメディアID111とが演算し、メディアユニークキーが導出される。メディアユニークキーがDESエンクリプタ142にてセッションキーKsによって暗号化され、DESエンクリプタ142の出力がホスト103のDESデクリプタ151に送信され、DESデクリプタ151によってメディアユニークキーが導出される。

【0115】

さらに、ドライブ102の乱数発生器143によってタイトルキーが生成され、乱数発生器143からのタイトルキーがホスト103のC2__E153に供給され、タイトルキーがメディアユニークキーを使用してC2によって暗号化される。暗号化タイトルキー114がメディア101に記録される。

【0116】

ホスト103において、セッションキーKsを鍵としてMAC演算ブロック158によりCCIのMAC値eKs(CCI)が計算され、CCIとともにドライブ102へ転送される。

【0117】

ドライブ102において、ホスト103から受け取ったCCIからセッションキーKsを鍵としてMAC演算ブロック157によりCCIのMAC値eKs(CCI)が計算され、ホスト103から受け取ったMAC値とともに比較159

へ供給される。

【0118】

比較159では、両方のMAC値が一致したならば、ホスト103から受け取ったCCIの改ざんは無いものと判断し、スイッチSW2をONする。一致しなかった場合は、CCIは改ざんされたものとみなし、スイッチSW2をOFFし、以降の処理を中断する。

【0119】

ドライブ102において、ホスト103から受け取ったCCIとタイトルキーとがC2__G145に供給され、コンテンツキーが導出される。コンテンツキーがDESエンクリプタ146に供給され、セッションキーKsを鍵として、コンテンツキーが暗号化される。暗号化コンテンツキーがホスト103のDESデクリプタ156に転送される。

【0120】

DESデクリプタ156でセッションキーKsを鍵として復号されたコンテンツキーがC2__ECBC155に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ113がドライブ102に転送され、ドライブ102によってメディア101に記録される。

【0121】

なお、図12に示すレコーダにおいては、タイトルキーがドライブ102の乱数発生器143によって生成されている。しかしながら、ホスト103側に乱数発生器を設け、この乱数発生器によってタイトルキーを生成しても良い。この場合には、生成されたタイトルキーがホスト103からドライブ102のコンテンツキー生成のためのC2__G145に対して転送される。

【0122】

図13は、レコーダの他の実施形態によるコンテンツ記録時の手順を示すものである。最初に、ホスト103からの要求に応じてメディア101上のMKBがシークされ、読み出される(ステップS61)。次のステップS62のAKEにおいて、リボーク処理とドライブ102とホスト103の相互認証動作がなされる。

【0123】

相互認証が成功しないと、リジェクト処理によって例えば処理が中断する。相互認証が成功すると、ドライブ102およびホスト103の両者において、セッションキー K_s が生成され、セッションキー K_s が共有される。

【0124】

次のステップS63において、ホスト103がドライブ102に対してメディアユニークキーを要求する。ドライブ102は、メディア101のメディアIDをシークし（ステップS64）、メディアIDをメディア101から読み出す（ステップS65）。ドライブ102は、メディアキーとメディアIDとを演算することによってメディアユニークキーを生成する。ステップS66において、メディアユニークキーがセッションキー K_s によって暗号化され、暗号化されたメディアユニークキーがホスト103に転送される。

【0125】

次に、ステップS67において、ホスト103がドライブ102に対してタイトルキーを要求する。ステップS68において、ドライブ102がタイトルキーをホスト103に転送する。ホスト103において、セッションキー K_s によって、暗号化されたメディアユニークキーが復号される。そして、タイトルキーがメディアユニークキーによって暗号化され、暗号化タイトルキーが生成される。

【0126】

また、ステップS69において、ホスト103がドライブ102に対してCCIを送る。このとき、CCIの改ざんを回避するためにCCIの認証データとして計算されたMAC値 $eK_s(CCI)$ を付加して転送する。ドライブ102において、CCIの改ざんが無いことを確認後、タイトルキーとCCIからコンテンツキーが生成され、コンテンツキーがセッションキー K_s で暗号化される。ステップS70において、ホスト103がドライブ102に対してコンテンツキーを要求すると、ステップS71において、ドライブ102が暗号化されたコンテンツキーをホスト103に送る。

【0127】

ホスト103は、暗号化コンテンツキーをセッションキー K_s によって復号し

、コンテンツキーを得る。コンテンツキーによってコンテンツが暗号化される。ステップS72において、ホスト103からドライブ102に対して、暗号化タイトルキー、暗号化コンテンツおよびCCIが転送される。ステップS73において、ドライブ102によって、暗号化タイトルキー、暗号化コンテンツおよびCCIがメディア101に対して記録される。

【0128】

上述した図12に示す構成のレコーダは、ドライブ102において、真正乱数またはそれに近い乱数をハードウェア例えばLSIによって発生することができ、生成した乱数を固定値への置き換えを困難とすることができる。また、ドライブ102において、ハードウェア構成によってコンテンツキーを生成するので、著作権保護の実装を強力とすることができる。

【0129】

この発明は、上述したこの発明の一実施形態等に限定されるものではなく、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えばタイトルキーは、タイトル毎のキーであるが、この発明では、乱数情報であれば、タイトル毎に異なることは、必要ではない。

【0130】

また、上述した説明においては、著作権保護技術としてCPRMおよびCPRMを拡張した例を挙げたが、CPRM以外の著作権保護技術に対してもこの発明を適用することができる。例えば、特開2001-352322号公報において提案されるツリー構造の鍵配布構成に基づく著作権保護技術に対して適用可能である。また、PCベースのシステムに対してこの発明が適用されるが、このことは、PCとドライブを組み合わせる構成にのみ限定されることを意味するものではない。例えば携帯型動画または静止画カメラの場合に、メディアとして光ディスクを使用し、メディアを駆動するドライブとドライブを制御するマイクロコンピュータが設けられる動画または静止画カメラシステムに対してもこの発明を適用することが可能である。

【0131】

【発明の効果】

この発明では、メディア上に記録された鍵情報（MKB）と各デバイスまたは各アプリケーションに記憶されている鍵情報（デバイスキー）から同一の値として導かれる鍵情報（メディアキー）を利用して相互認証がなされる。したがって、この発明においては、認証のためだけに用意される特定の認証鍵を必要とせず、秘密情報を少なくでき、また、デバイスまたはアプリケーションによってデバイスキーを異ならせることが可能であるので、秘密情報が不正に読み取られる危険性を少なくできる。

【0132】

この発明では、著作権保護技術に関する秘密情報である電子機器またはアプリケーションソフトウェア固有の情報例えばデバイスキーがドライブ内に実装されているので、情報処理装置にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報の全てを持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持たせることが容易に実施でき、また、ディスクからのデータとしてそのまま読み出された暗号化コンテンツが「DeCSS」のような解読ソフトウェアにより復号され、平文のままのクリア・コンテンツとしてコピー制限の働かない状態で複製が繰り返されるような事態を防ぐことができることから、著作権保護技術の安全性を確保することができる。

【0133】

また、電子機器固有の情報としてのデバイスキーを記録再生装置が持つことによって、記録再生装置自身をリボークすることが可能となる。

【0134】

さらに、この発明では、情報処理装置におけるコンテンツキーを計算するのに必要とされる乱数情報が記録再生装置内の例えばLSIによって生成できるので、PC内でソフトウェアによって乱数を生成するのと比較して、真正または真正乱数に近い乱数を生成することができる。したがって、乱数が固定値に置き換えられる、等のおそれを少なくできる。

【図面の簡単な説明】

【図1】

先に提案されているレコーダ、プレーヤおよびDVDメディアからなるシステムを説明するためのブロック図である。

【図 2】

PCベースのDVDメディア記録再生システムを説明するためのブロック図である。

【図 3】

図 2 のシステムにおけるDVDドライブ 4 およびホスト 5 の処理の手順を説明するための略線図である。

【図 4】

図 2 のシステムにおける認証動作を説明するためのフローチャートである。

【図 5】

この発明の一実施形態による相互認証のための構成を示すブロック図である。

【図 6】

この発明の一実施形態におけるドライブの認証動作の処理の手順を説明するためのフローチャートである。

【図 7】

この発明の一実施形態におけるホストの認証動作の処理の手順を説明するためのフローチャートである。

【図 8】

この発明の一実施形態によるドライブとホストを組み合わせたレコーダの構成の一例をブロック図である。

【図 9】

レコーダの一例の通信の手順を説明するための略線図である。

【図 10】

この発明の一実施形態によるドライブとホストを組み合わせたプレーヤの構成の一例をブロック図である。

【図 11】

プレーヤの一例の通信の手順を説明するための略線図である。

【図 12】

この発明の一実施形態によるドライブとホストを組み合わせたレコーダの構成の他の例をブロック図である。

【図 13】

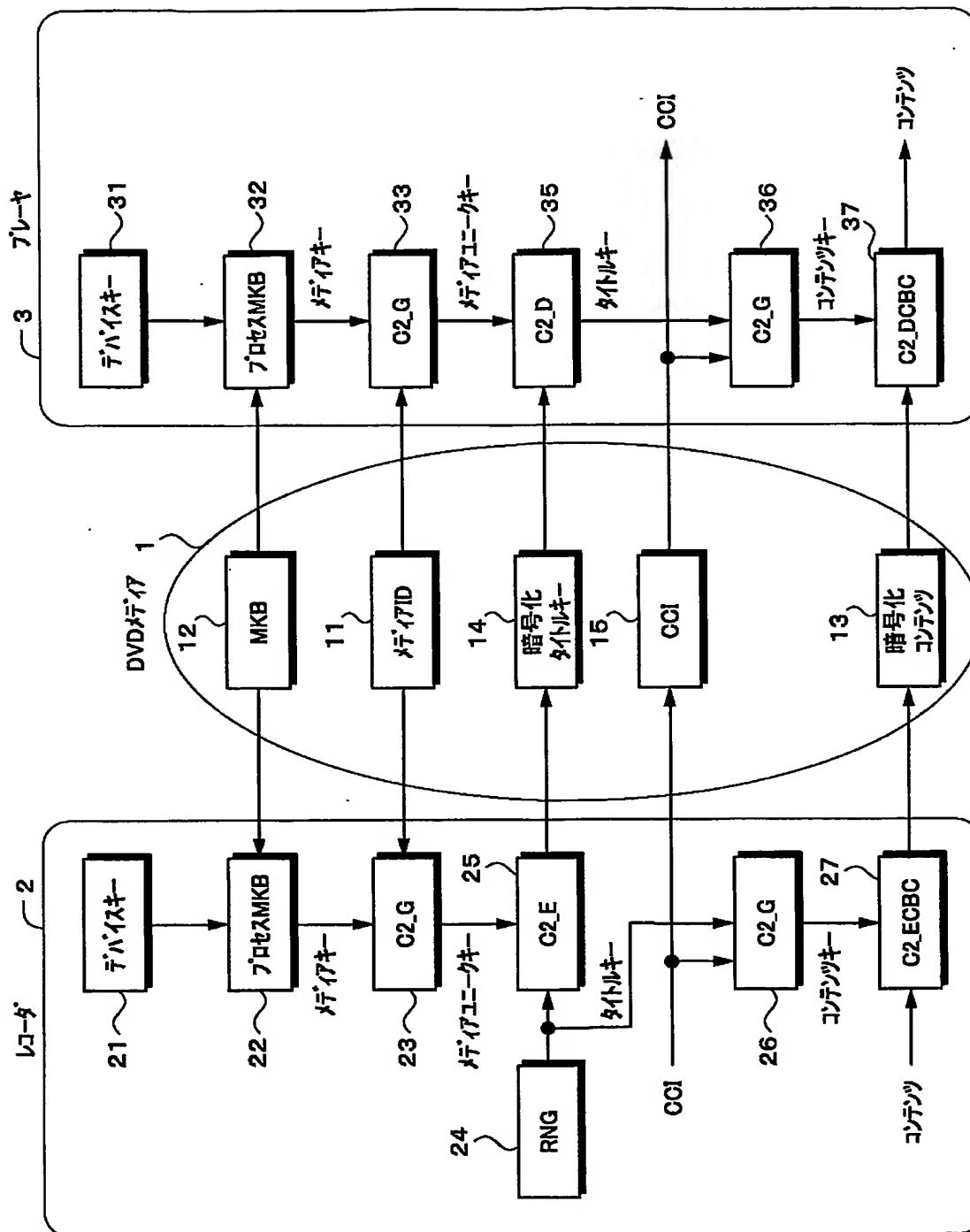
レコーダの他の例の通信の手順を説明するための略線図である。

【符号の説明】

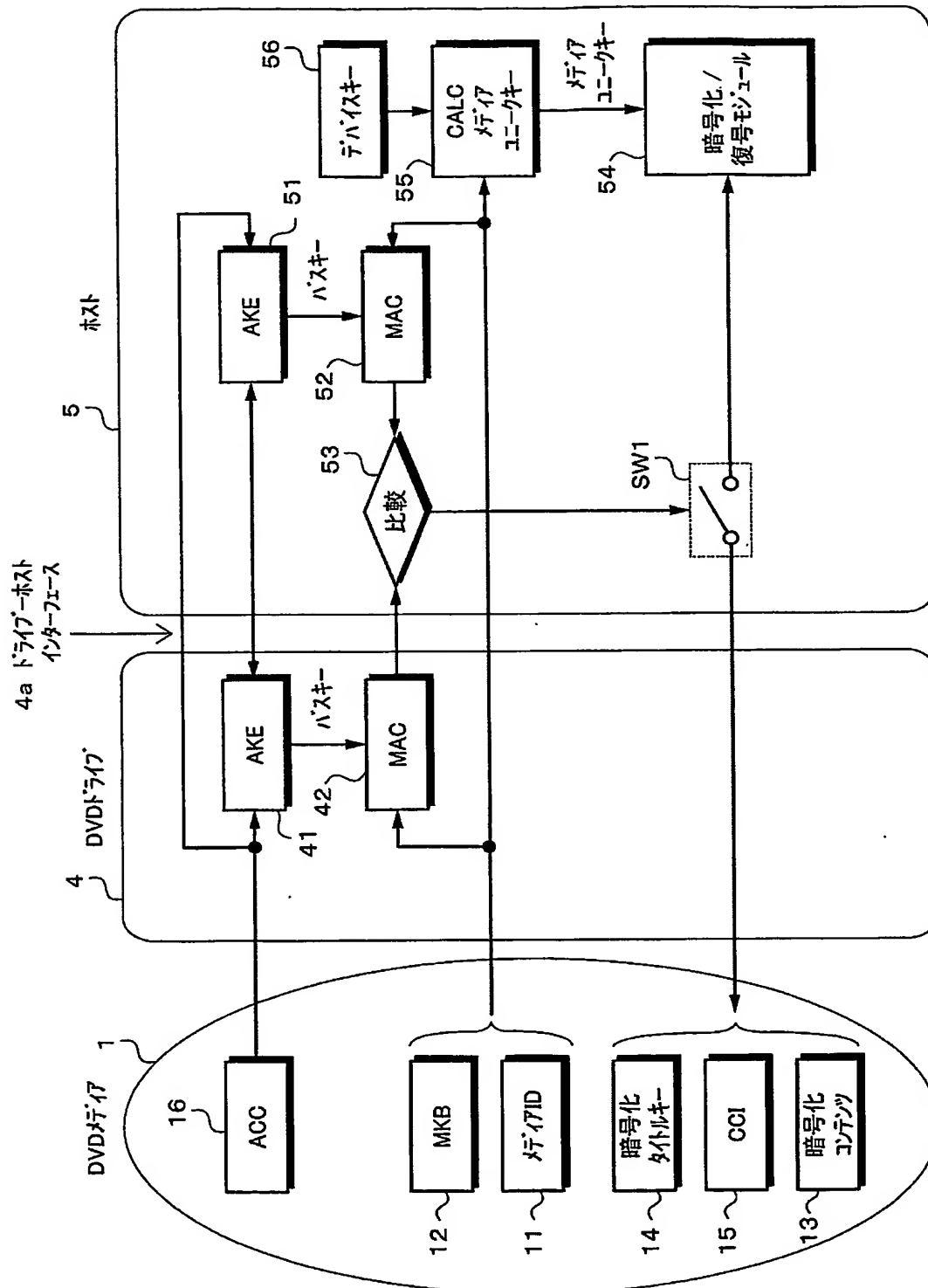
1・・・DVDメディア、2・・・レコーダ、3・・・プレーヤ、4・・・DVDドライブ、4a・・・インターフェース、5・・・ホスト、11・・・メディアID、12・・・メディアキーブロック(MKB)、13・・・暗号化コンテンツ、42, 52・・・MAC演算ブロック、46・・・デバイスキー、46a・・・デバイスキーの前半部、47・・・DESエンクリプタ、48・・・メディアユニークキー演算ブロック、49, 49a・・・DESエンクリプタ、49b・・・DESデクリプタ、53・・・MACを比較する比較、54・・・暗号化/復号モジュール、55・・・メディアユニークキー演算ブロック、101・・・メディア、102・・・ドライブ、103・・・ホスト、104・・・インターフェース、121・・・ドライブのデバイスキー、122・・・プロセスMKB、123, 124, 125・・・ドライブのMAC演算ブロック、126, 127, 128・・・ドライブの乱数発生器、129・・・比較、131・・・ホストのデバイスキー、132・・・プロセスMKB、133, 134, 135・・・ホストのMAC演算ブロック、136, 137, 138・・・ホストの乱数発生器、139・・・比較、141, 154・・・C2__G、142, 144・・・DESエンクリプタ、143・・・乱数発生器、151, 152, 156・・・DESデクリプタ、153・・・C2__E、155・・・C2__EBC、157, 158・・・MAC演算ブロック、159・・・比較

【書類名】 図面

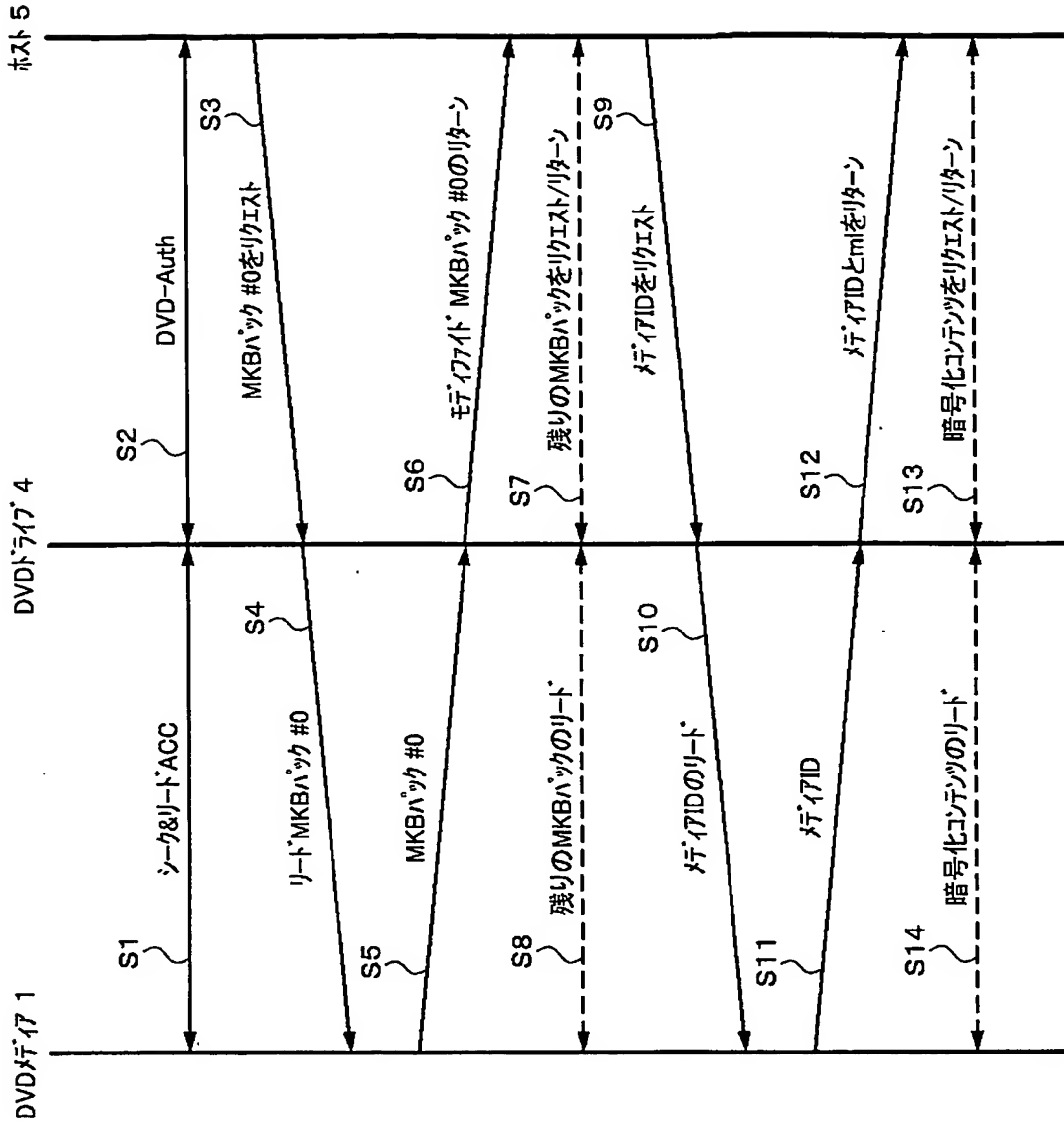
【図1】



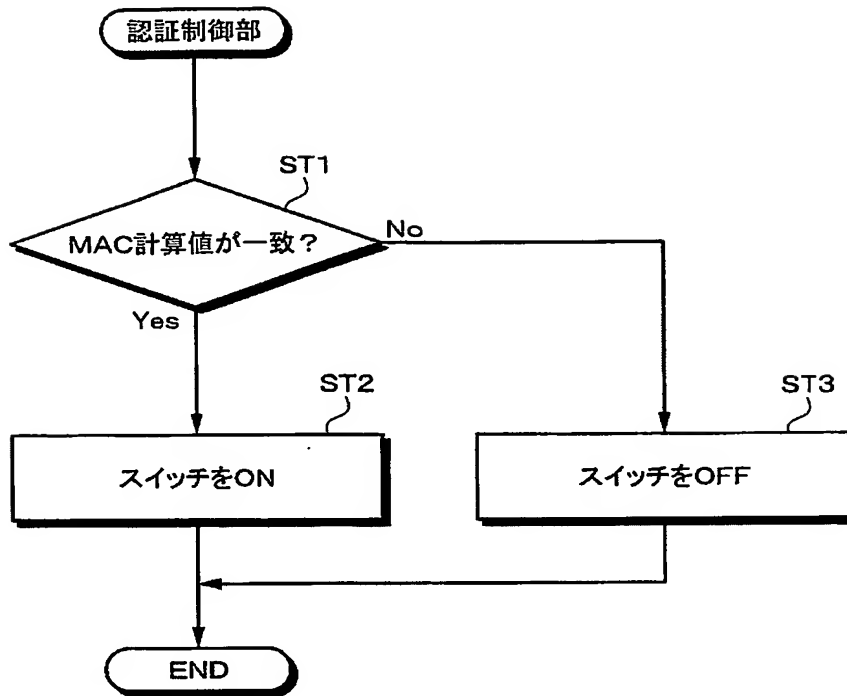
【図2】



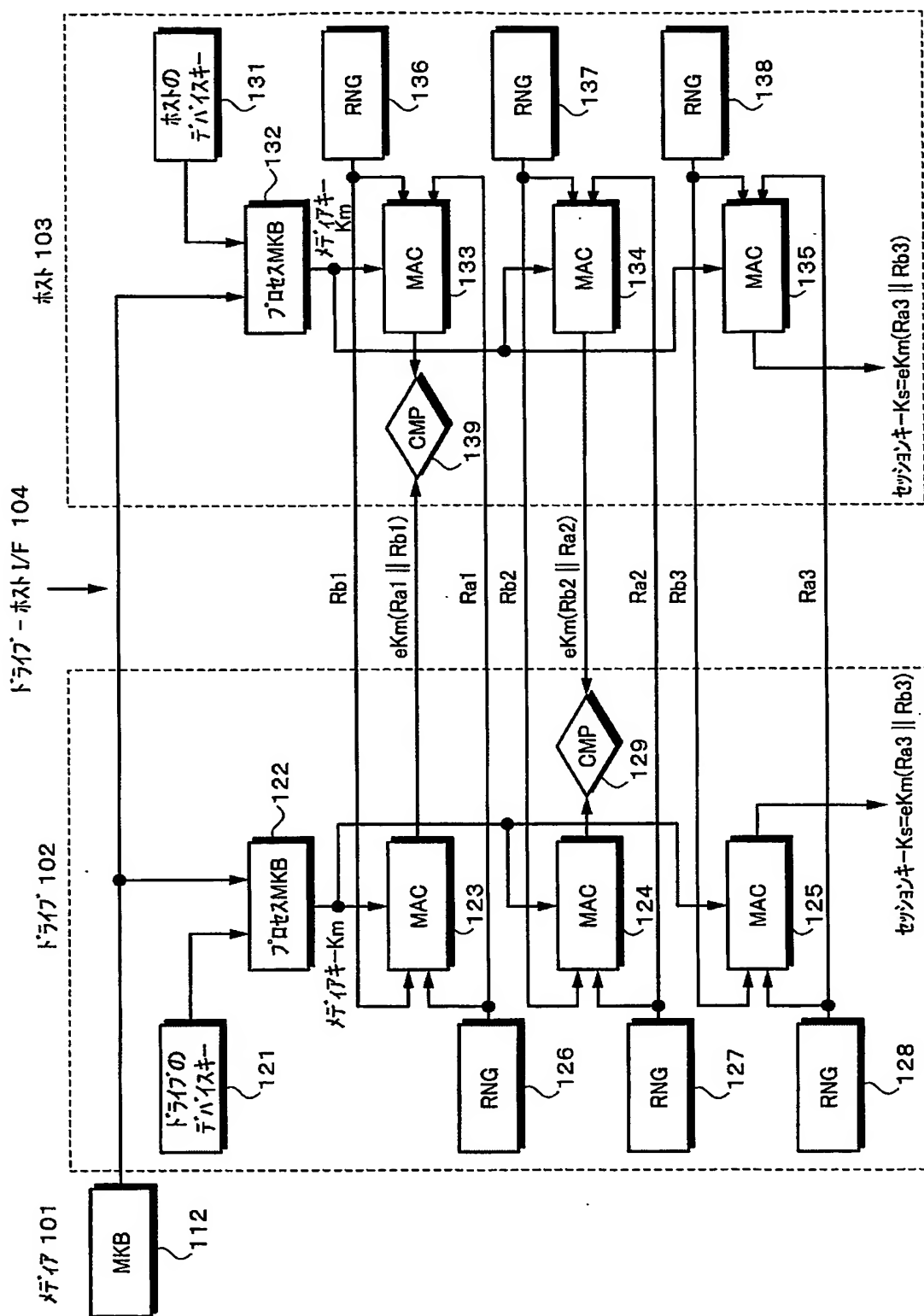
【図 3】



【図 4】

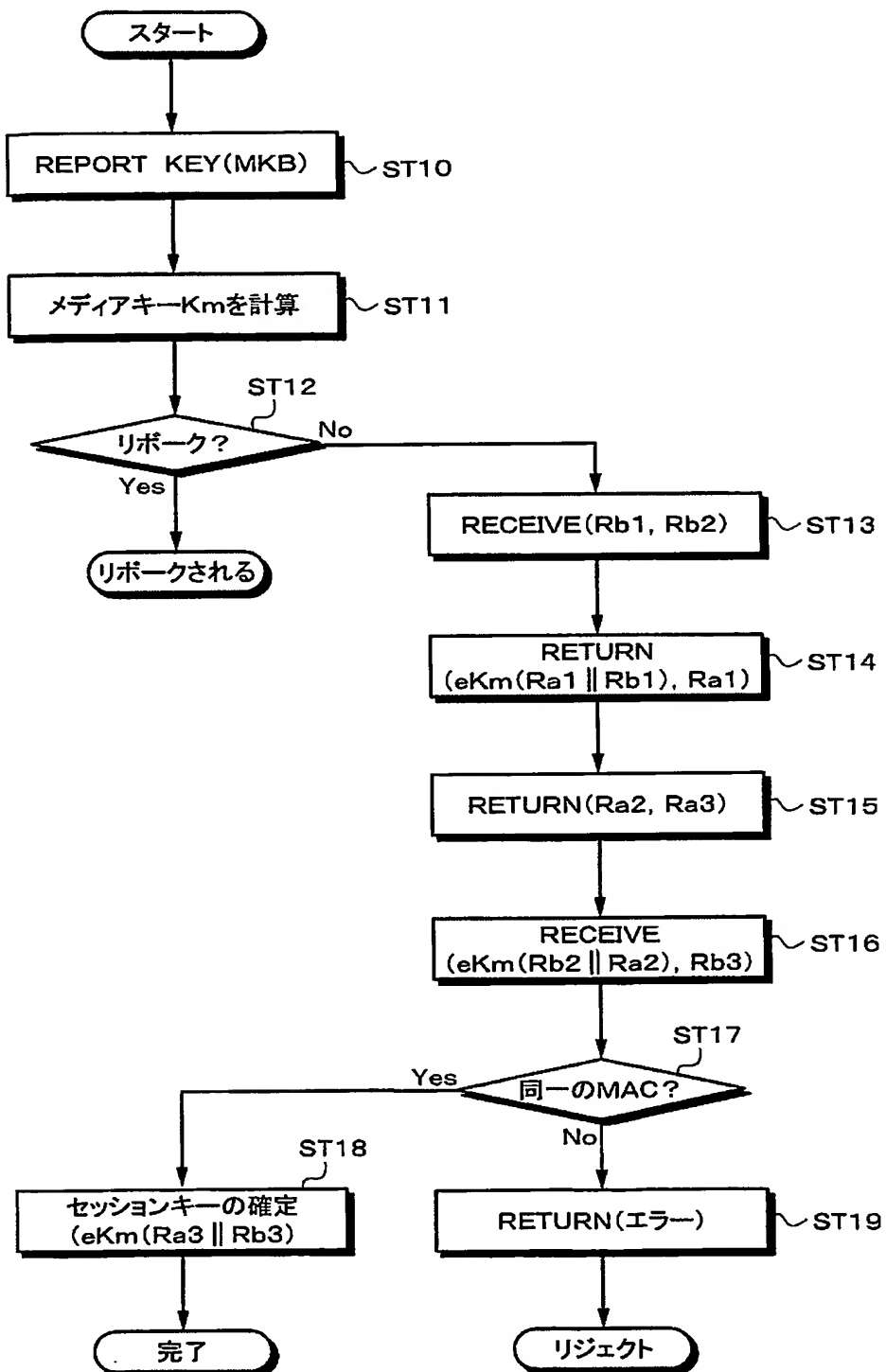


【図 5】

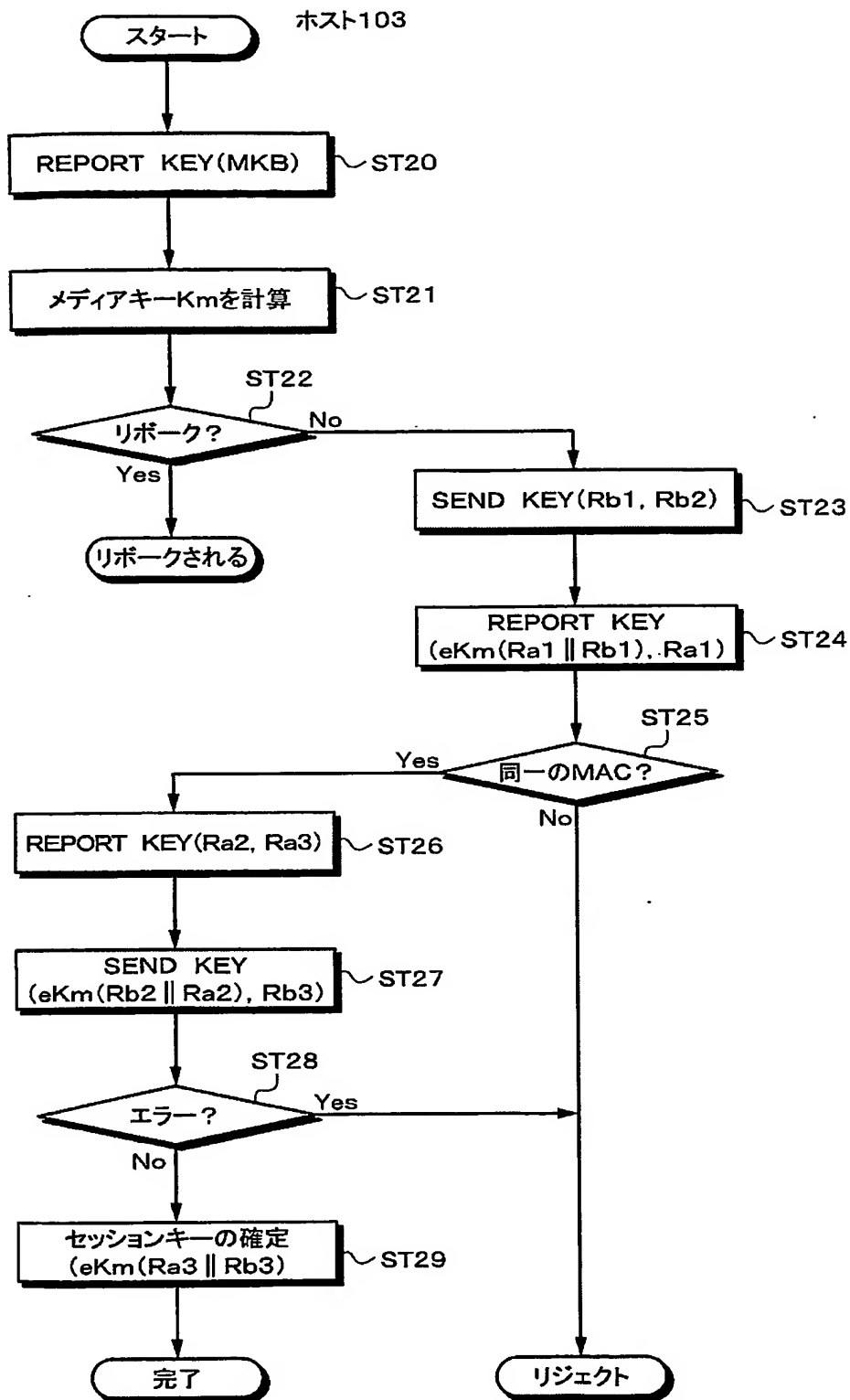


【図6】

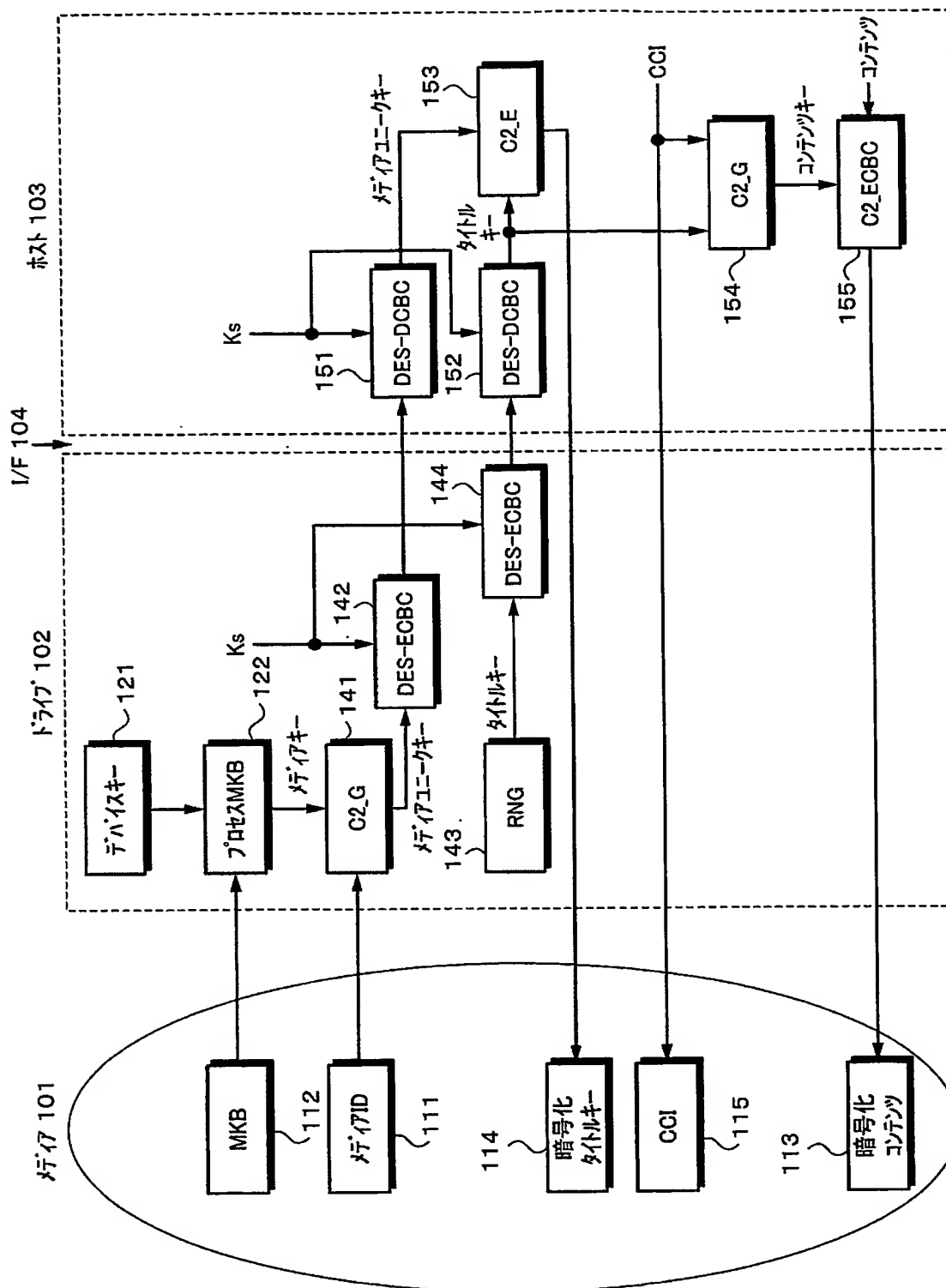
ドライブ102



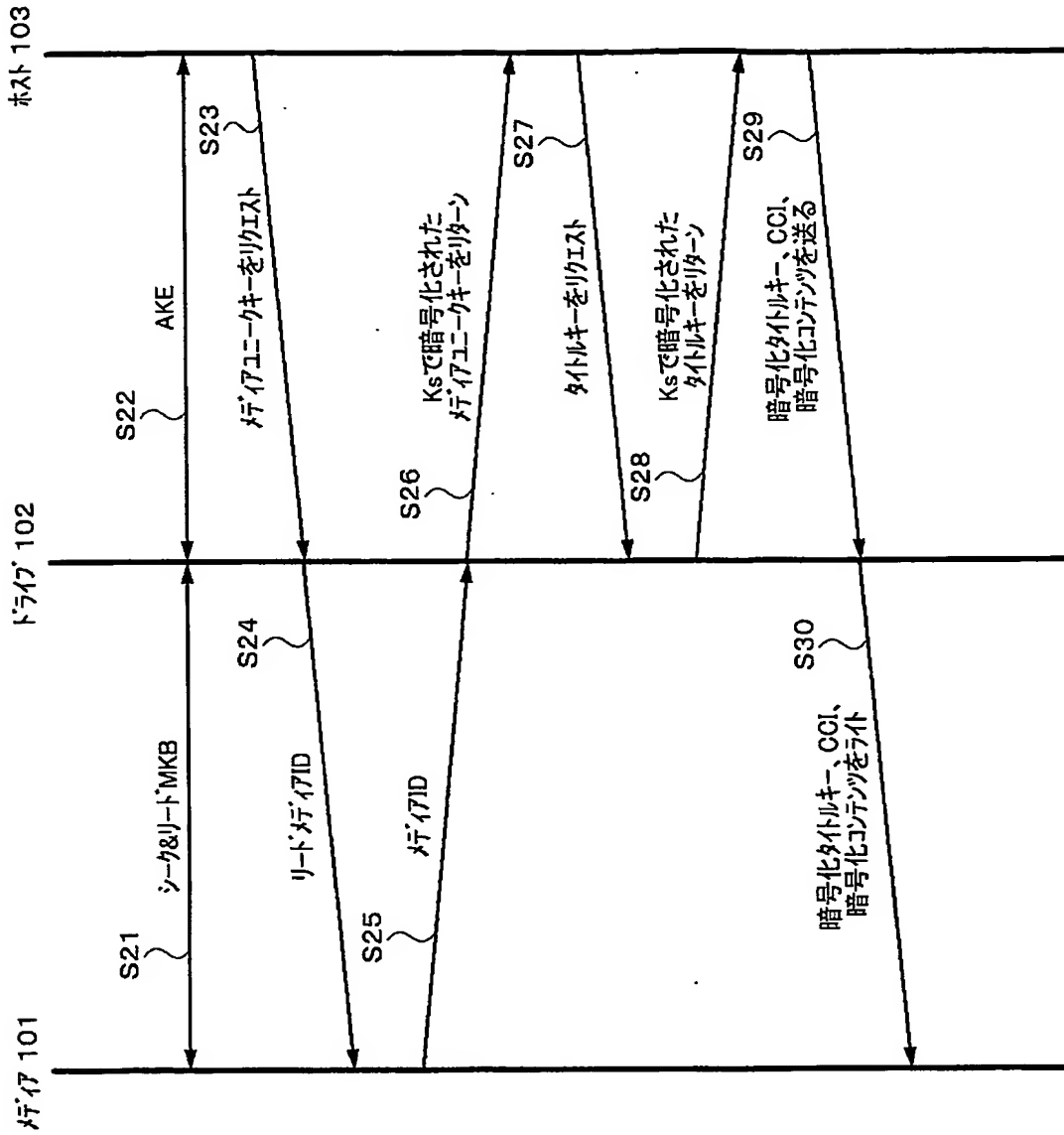
【図7】



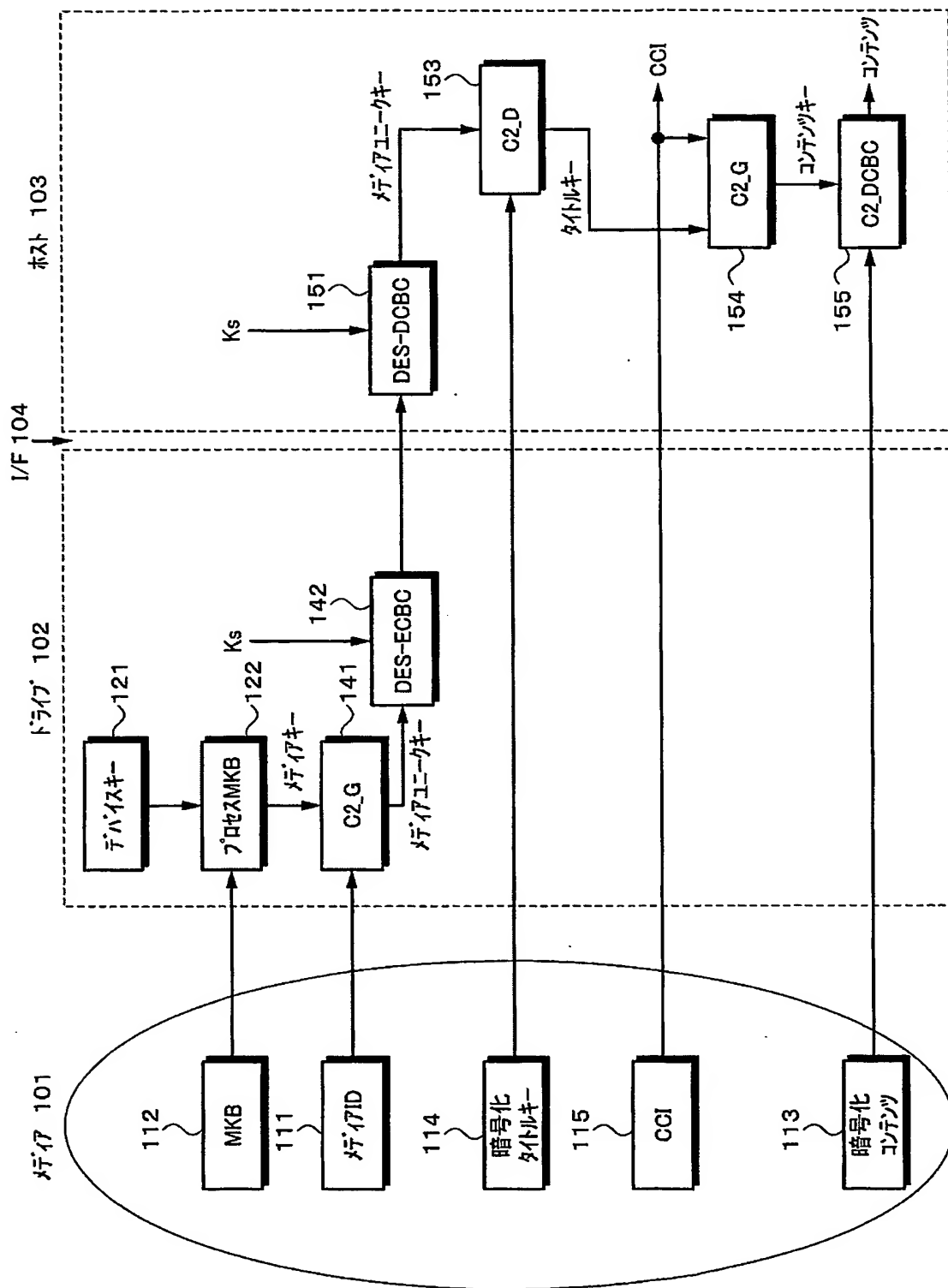
【図 8】



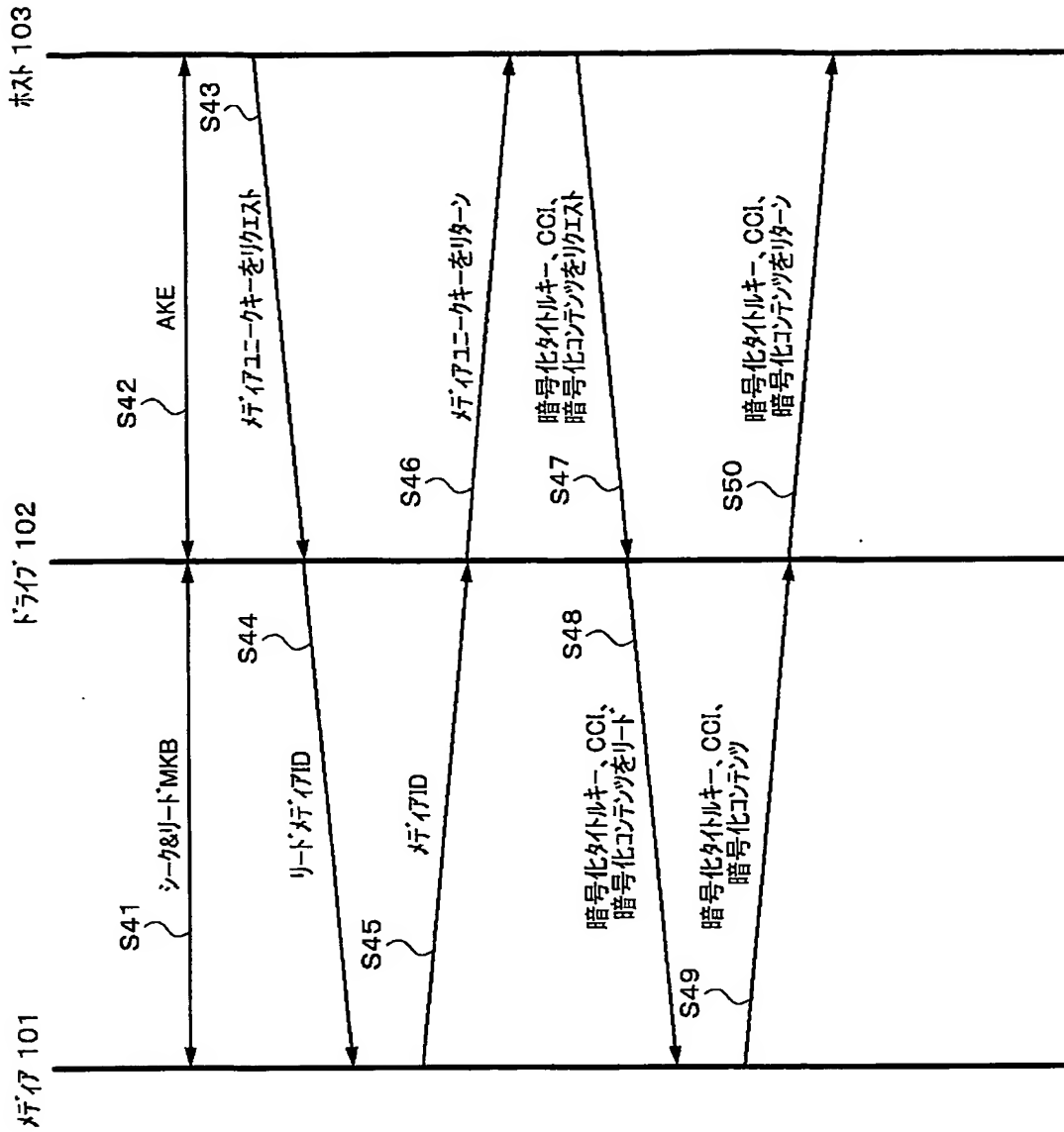
【図 9】



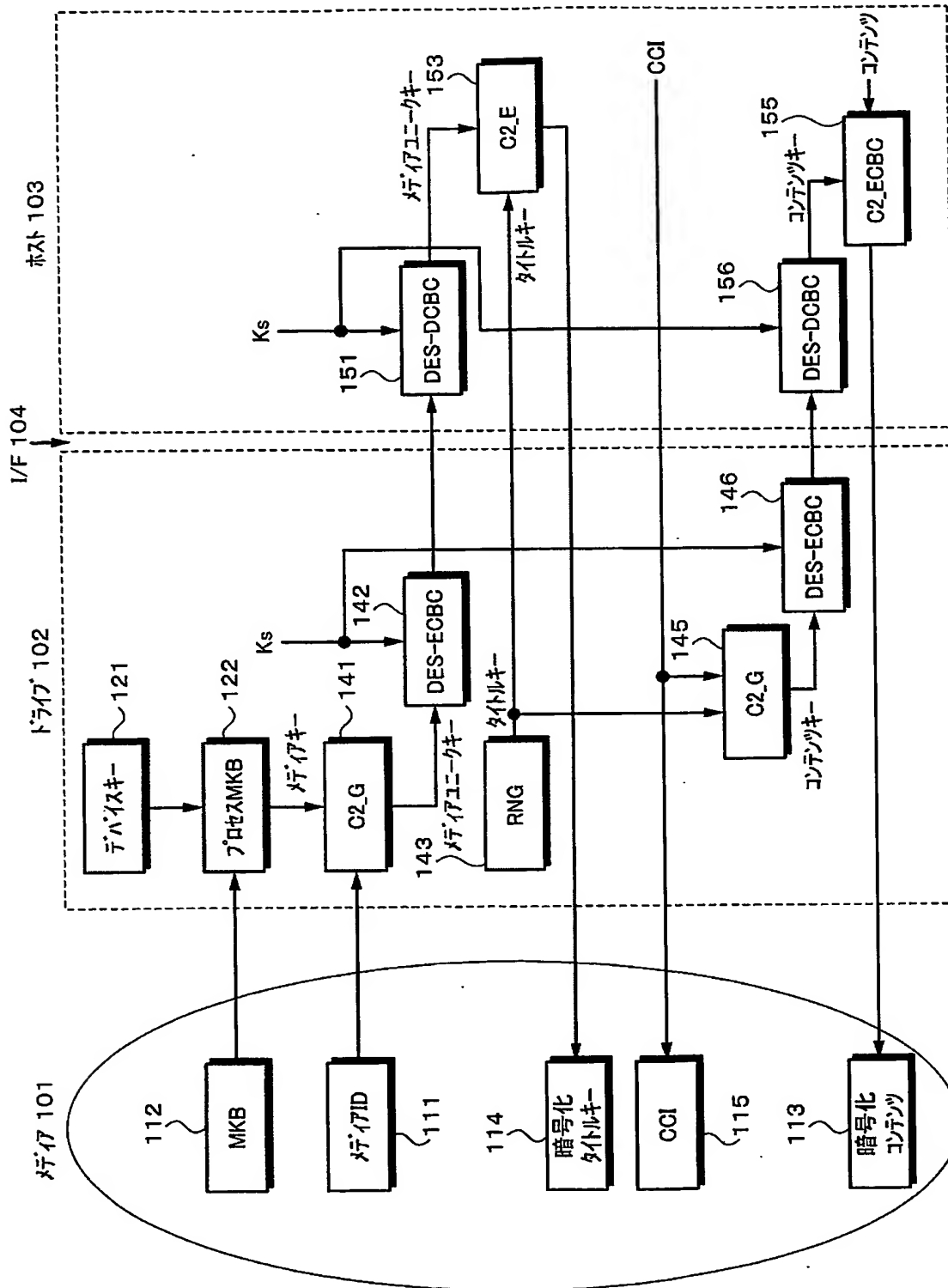
【図 10】



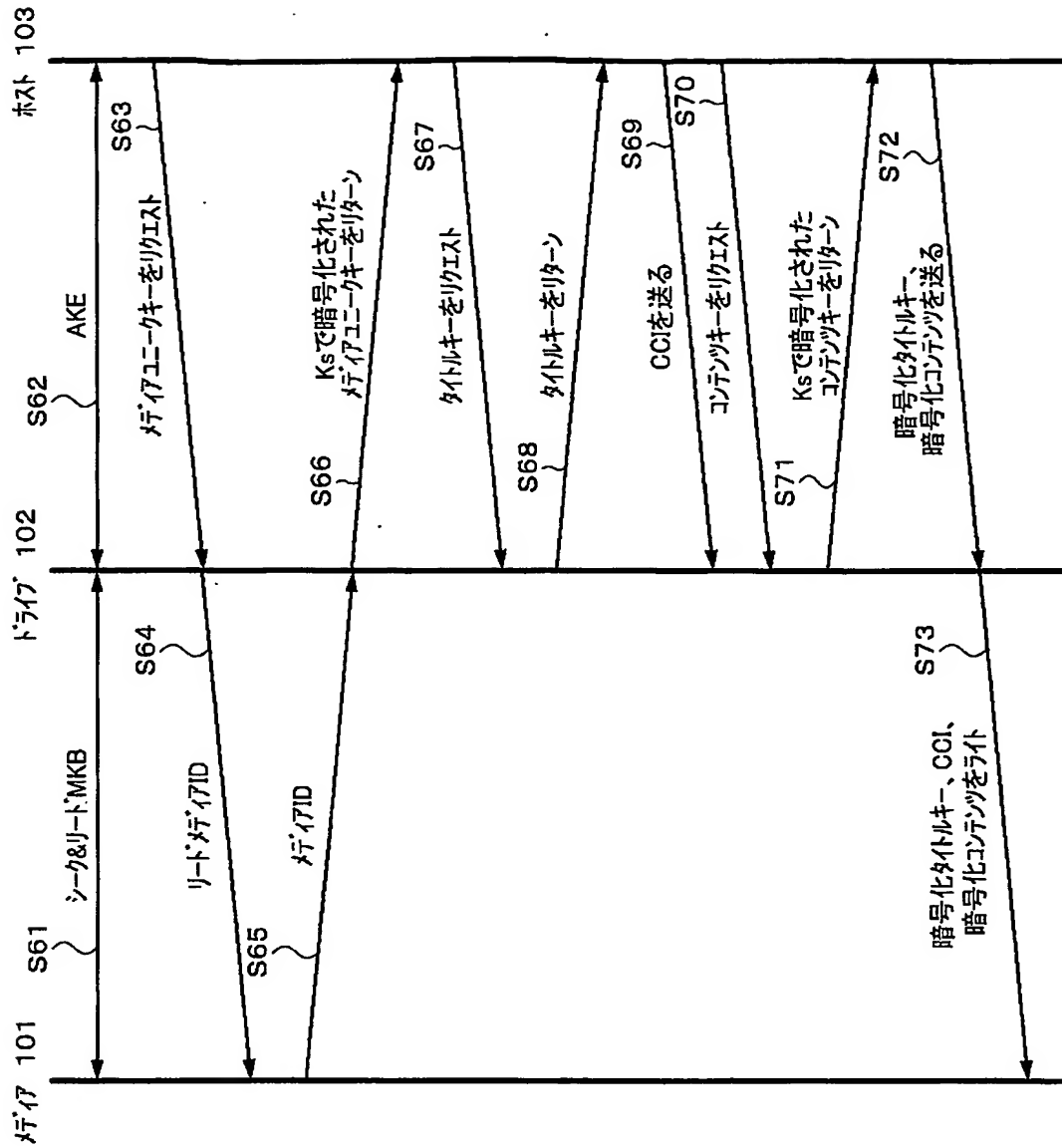
【図 11】



【図 12】



【図13】



【書類名】 要約書

【要約】

【課題】 著作権保護技術の安全性を高め、また、違法なドライブ等の電子機器をリボークする。

【解決手段】 プロセスMKB122にMKBとドライブの持つデバイスキー121とが入力され、ドライブがリボーク処理され、プロセスMKB132によってホスト103がリボーク処理される。MAC演算ブロック123および133が演算したMAC値がホスト103内において比較され、二つの値が同一と判定されると、ホスト103によるドライブ102の認証が成功したことになる。ホスト103のMAC演算ブロック134および124が演算したMAC値がドライブ102内において比較され、二つの値が同一と判定されると、ドライブ102によるホスト103の認証が成功したことになる。相互認証が成功すると、MAC演算ブロック125および135によって、共通のセッションキーが生成される。

【選択図】 図5

特願 2 0 0 3 - 0 0 6 9 1 5

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 2 1 8 5]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都品川区北品川 6 丁目 7 番 3 5 号

氏 名

ソニー株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.